PRIVACY POLICY

This Policy applies to Everyday Independence Pty Ltd (EI), a subsidiary of APM Human Services International Pty Ltd (APM Group).

EI's collection, use, disclosure and storage of your personal information is regulated by the *Privacy Act 1988* (Cth), the Australian Privacy Principles and related legislation.

Updates to this Privacy Policy will be published on our website.

If you have any questions regarding this Policy or our privacy practices generally, please do not hesitate to contact our Privacy Officer at privacy@everydayind.com.au.

Purpose

The purpose of this Privacy Policy is to:

- Give you an understanding of the kinds of personal information that we collect and hold.
- Communicate how and when your personal information is collected, disclosed, used, held and otherwise handled by us.
- Inform you about the purposes for which we collect, hold, use and disclose personal information.
- Provide you with information about how you may access your personal information and seek correction of your personal information.
- Provide you with information about how you may make a complaint, and how we will deal with any such complaint.

Policy Statement

We are strongly committed to maintaining the privacy of personal information we collect as part of the services we offer. We place great importance on protecting the privacy of our employees/contractors, valued clients, customers and other stakeholders.

What is personal information?

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not. It includes your name, date of birth / age, gender and contact details as well as health information (which is also sensitive information). In this privacy policy, a reference to personal information includes sensitive / health information.

Collection of personal information

Personal information collected by us will usually fall into one of the following categories:

- Contact information (name, age, address, email address and telephone numbers).
- Emergency contact information.
- Commonwealth identifiers (such as your National Disability Insurance Scheme (NDIS) reference number, your Medicare number or your Tax File Number).
- Employment information (such as employment history, work performance, emergency contact details, absences and workplace incidents).
- Financial information (such as your bank account details and credit card details).
- Sensitive information (such as information about your disability, health condition, medical history, assessment questionnaires and outcomes, criminal history, religious beliefs, cultural background, trade union activity).
- Photos and video footage of your treatment with us (where express consent received).

We may collect personal information about:

- clients;
- parents, guardians and/or carers of clients and other family members of clients (where applicable);
- teachers of clients (where applicable);
- healthcare professionals in the course of them referring clients to us and/or providing
- information to us about your condition and treatment, or in the course of us engaging them to assist us to provide services to our clients;
- third parties providing a service to us; and
- employees, contractors, students and volunteers.

We may collect your information from you in a variety of ways including when:

- we provide services to you;
- you visit our website;
- you submit your information in response to EI marketing events or activities; or
- you contact us by any method, such as face-to-face, over the telephone, through an online form or portal, through a paper form or by email.

Sometimes we will collect personal information from a third party or a publicly available source, for example where we have your consent, where we are required by law to do so, or if it is unreasonable or impracticable to collect the personal information directly from you (e.g. checking a candidate's work history, or obtaining client information from a parent, guardian or carer (where applicable), or from your treating healthcare professionals). The Client Consent Form more specifically outlines where client-related personal information might be collected from.

You may choose to deal with us anonymously or under a pseudonym where lawful and practical. Where anonymity or the use of a pseudonym will render EI unable to provide the relevant service or reasonably conduct business, we may request that you identify yourself.

You may also choose not to provide us with your personal information. Depending on the circumstances in which you do so, however, we may be unable to provide you with our services as a result.

Where we are collecting personal information from a child or young person, we will use our judgement to determine if that person has the capacity to consent. Where we are unsure, we will seek consent from a parent, guardian or carer.

Why do we collect, use, disclose and store your personal information?

We collect, use, disclose and store your personal information to provide you with our services which include:

- speech and language pathology, occupational therapy, physiotherapy, positive behaviour support, habit coaching, early childhood supports and developmental education;
- invoicing and processing any fees payable in relation to the services rendered;
- managing our relationship with you (including if you are a health professional, client, service provider, employee, contractor, student or volunteer) and to contact you for follow up purposes;
- providing you with information about our services (and services offered by other members of the APM Group) including our news updates and information about events;
- with your consent, for NDIS auditing purposes;

- verifying and updating personal information held by us;
- recruiting, managing, training and clinically supervising personnel (including employees, contractors, students and volunteers);
- reviewing, developing and improving our services, as well as our business, operational and IT processes and systems;
- resolving any complaints and issues;
- complying with our legal or regulatory obligations; and
- for other purposes required or authorised by or under law, including purposes for which you have provided your express or implied consent.

We may also collect, use and store your personal information:

- for marketing purposes, in order to provide you information about the services we and the APM Group offer;
- to respond to your questions and suggestions;
- to improve the quality of your visit to our website;
- to undertake employee recruitment activities; or
- to assist with data analytic processes.

You may opt out of receiving marketing information by notifying us accordingly, or by using any unsubscribe facility we provide for that purpose. If you opt out of receiving marketing information, we may still contact you in connection with the services we provide to you, such as for appointment reminders and follow-ups.
Our services, functions and activities, as well as those of our contracted service providers, may change from time to time.

Protecting and storing your personal information

We understand the importance of keeping personal information secure and safe. Some of the ways we do this are:

- Requiring employees and contractors to enter into confidentiality agreements;
- Securing hard copy document storage (i.e. storing hard copy documents in locked filing cabinets);
- Implementing security measures for access to computer systems to protect information from unauthorised access, modification or disclosure and loss, misuse and interference;
- Ensuring data storage devices such as laptops, tablets and smartphones are password protected;
- Providing discreet environments for confidential discussions;
- Implementing access control for our buildings including waiting room / reception protocols and measures for securing the premises when unattended; and
- Implementing security protocols for our website.

Personal information may be stored in documentary form but will generally be stored electronically on our software or systems.

We will take reasonable steps to ensure that personal information that is held which is no longer required, including under any contractual or legal requirement, is destroyed or de-identified in a secure manner.

Who may we disclose your personal information to?

In order to carry out our services, functions and activities, EI may disclose your personal information to third party suppliers or contractors such as cloud computing technology and data storage service

providers, data analytic and marketing services, legal services providers, insurance brokers, security service providers, business advisors and financial service providers. We may disclose personal information to these third parties in connection with their provision of goods or services to us. In addition, we may share your personal information with other APM Group entities for promotional purposes including direct marketing.

We may also disclose your personal information to government agencies, private sector organisations or other entities where required or permitted by law, which may include the following circumstances:

- You have consented to such disclosure.
- We believe that you would reasonably expect, or have been told, that information of
- that kind is usually passed to those individuals, bodies or agencies, and it is being disclosed for a purpose related (or directly related, in the case of sensitive information) to the reason we collected the information.
- We are required or authorised to make such disclosure by law or the requirements of any professional bodies, including where we are required to do so in accordance with child safety obligations.
- A permitted general situation or permitted health situation (as these terms are defined in the Privacy Act) exists in relation to the disclosure.
- We believe it is reasonably necessary for enforcement related activities conducted by, or on behalf of, an enforcement body (e.g. police, ASIC, Immigration Department).

Information is shared between APM Group Members. We may transfer or disclose your personal information to APM Group members.

The persons and organisations which EI may disclose your personal information to will handle your personal information in accordance with their privacy policies.

Will my personal information be disclosed overseas?

The persons to whom we disclose personal information are normally located in Australia, although personal information related to our staff and for our marketing activities may be disclosed to recipients outside Australia. We may also use digital technology service providers whose operations are located overseas (such as the providers of customer management system integrations in the United States of America). In all instances where this occurs, we will act in accordance with the Privacy Act and this Privacy Policy.

Accuracy of Personal Information

We take steps to help ensure that all personal information we collect, use or disclose is accurate, complete and up to date. Please contact the EI Privacy Officer (details below) if you are aware that personal information that we hold about you does not meet this objective.

How can I access or correct my personal information and contact Everyday Independence?

You can request access to personal information that we hold about you.

The procedure for requesting and obtaining access is as follows:

- All requests for access to personal information to be made in writing and addressed to our Privacy Officer (see contact details below). All requests should specify how the information is proposed to be accessed (photocopies, electronic copy, or visual sighting).
- Please provide as much detail as possible regarding the EI business, department and / or person to whom you believe your personal information has been provided and when. This will allow us to process your request more efficiently.
- We will endeavour to acknowledge your request within 14 days of the request being made.
- Access will usually be granted within 30 days of our acknowledgment. If the request cannot be processed within that time for whatever reason, we will let you know the anticipated timeframe for a response to be provided.
- You will need to verify your identity and authority before access to personal information is granted.
- We may charge a reasonable fee for access to personal information, which will be notified and required to be paid prior to the release of any information. Once the request has been processed by
- us, you will be notified of our response and proposal for suitable access (provision of photocopies, digital copies or visual sighting, where appropriate).
- We may refuse to grant access to personal information if there is an exception to such disclosure which applies under relevant privacy legislation.
- If, as a result of access being granted, you are aware that we hold personal information that you regard as being no longer accurate or correct, you may request the deletion or correction of such information.
- Upon receipt of a request to correct or delete personal information, we will either make such corrections or deletions or provide written reasons as to why we declined to make such alterations.

We have a designated Privacy Officer who is responsible for the management of:
- Requests for access to personal information.
- Complaints regarding our management of personal information.

For information regarding privacy, our Privacy Officer can be contacted at:
E: privacy@everydayind.com.au
A: 58 Ord Street, West Perth WA 6005
P: 1300 179 131

How do we handle complaints?

If you have any concerns or complaints about the way your personal information has been collected or handled by EI, please advise us of your concern or complaint in writing and send it to the Privacy Officer using the contact details above. EI will endeavour to acknowledge receipt of a written complaint within 5 business days.

EI's Privacy Officer will investigate the complaint and attempt to resolve it within 20 business days after the written complaint was received. Where it is anticipated that this timeframe is not achievable, we will try to contact the person making the complaint to provide an estimate of how long it will take to investigate and respond to it.

It is our intention to use our best endeavours to resolve any complaint to your satisfaction. However, if you are unhappy with our response, you may contact the Office of the Australian Information Commissioner and/or the relevant privacy regulator in your State/Territory who may investigate your complaint further.