PRIVACY POLICY

PURPOSE

Arriba Group Pty Ltd (Arriba Group) is committed to respecting an individual's right to privacy. This policy explains the ongoing responsibilities of Arriba Group regarding the handling of personal information.

SCOPE

This policy covers personal information collected or managed about individuals interacting with Arriba Group or its controlled entities including clients we support, prospective employees applying for employment opportunities and contractors. This policy covers Rehab Management (Aust) Pty Ltd, LiveBig Pty Ltd, AimBig Employment Pty Ltd and OneRedDoor Pty Ltd.

Arriba Group collects, uses, discloses and stores personal information in accordance with the Privacy Act (Cth), the Australian Privacy Principles (APPs), and relevant State and Territory legislation applicable to its operations. NDIS providers follow the NDIS Code of Conduct and the NDIS Practice Standards.

OUR POLICY

Arriba Group acknowledges and respects individuals' right to privacy. In doing so, The Arriba Group is committed to protecting personal information. We take all reasonable steps to ensure compliance with Australian Privacy Laws and to address related enquiries and complaints, including mandatory training for all staff.

Arriba Group may update this privacy policy periodically to reflect changes in laws, technology, or our practices and operations. We will post the updated version of the policy on our website.

Arriba Group recognises the opportunities and importance of adopting Artificial Intelligence (AI) as a valuable and innovative tool in supporting and enhancing the delivery of its services, business strategies and the achievement of its overall vision and mission. The group strives to ensure that it is done in a safe, ethical and responsible manner. We support the Australian Government's AI Ethic Principles including AI systems that respect and uphold privacy rights and data protection and ensure the security of data. We also support transparency and responsible disclosure so people can understand when they are being significantly impacted by AI and can find out when an AI system is engaging with them.

Individuals have the right to complain if they believe their privacy has been breached. The procedure for making a complaint and how complaints are dealt with is outlined below.

For questions or feedback about this policy, contact us at:

Privacy Officer
Arriba Group
Suite 15.04, level 15/680
George Street
Sydney NSW 2000
T 1300 762 989
Email: privacy.officer@arribagroup.com.au

COLLECTION OF PERSONAL INFORMATION

What is Personal Information?

Personal Information is information or an opinion that identifies an individual. Examples of Personal Information we collect includes names, addresses, email addresses, phone and facsimile numbers. It includes a person's name, date of birth / age, gender and contact details as well as health information (which is also sensitive information). In this policy, a reference to personal information includes health (sensitive) information.

What personal information do we collect and hold?

We collect personal information only when necessary for our functions or activities. We may collect the following types of personal information:

- Name
- Mailing or street address
- Email address
- Telephone number
- Facsimile number
- Age or birth date
- Profession, occupation or job title

For clients and prospective clients, we may also collect health information, employment information and other sensitive information for the purpose or providing high-quality services. For people who visit our websites we may also collect information about the pages visited, language preferences, interactions and search activities.

For job applicants or contractors, we may also collect information on person's job application, professional development history, salary and payment information, including superannuation details, medical information (e.g. details of disabilities and/or allergies, medical certificates), and workplace surveillance information. For contractors who are assigned one of

our work email addresses, we may maintain records regarding use of our ICT resources, such as emails and internet activity.

In some circumstances we record telephone conversations for quality, compliance and training purposes. If an individual prefers not to have their conversation recorded, please inform our staff.

We do not adopt, use or disclose government-related identifiers (such as Medicare or tax file numbers) except as permitted by law.

Why do we collect, use and store personal information?

We collect personal information for the primary purpose of providing our services, providing information to our clients and marketing, for example sending information updates and newsletters. We may also use personal information for related secondary purposes that would reasonably be expected. An individual can unsubscribe from our mailing/marketing lists at any time by clicking the unsubscribe link in our emails or by contacting us directly.

When we collect personal information, we will, where appropriate and where possible, explain why we are collecting the information and how we plan to use it.

For clients and prospective clients, we also collect, hold, use and disclose personal information for the following purposes:

- providing information and updates about our services
- assessing eligibility for our services and determining how we can best help
- providing services to individuals, which in some cases may include health services
- researching, monitoring and evaluating our services so we can continue to improve the quality and outcomes of our services as well as develop new services
- advocating for the improvement of service quality and outcomes

- meeting our funding, professional and legal obligations (including our duty of care) in providing our services
- processing and responding to complaints
- providing information to third parties as authorised or required by law
- sending newsletters (unless a person chooses not have newsletters sent to them).
- sending information and updates about other services of Arriba Group.

For job applicants and contractors to Arriba Group, we also collect, hold, use and disclose personal information to establish and maintain a relationship and to fulfill our duties under this relationship. Personal information will not be shared, sold, rented or disclosed other than as described in this policy.

How do we collect personal information?

When we are collecting personal information, we collect it in several ways including:

- through access and use of our websites and online presence
- during correspondence between individuals and our representatives
- through application forms or purchase orders.

Where reasonable and practicable, Arriba Group will collect personal information directly from the individual. In certain circumstances, information may be obtained from third parties. If this occurs, the organisation will take reasonable steps to inform the individual about the information received from those third parties.

When collecting personal information, Arriba Group will take reasonable steps to inform individuals about its purpose, intended use, and potential disclosure.

In most cases, Arriba Group will require individuals receiving services (or their legal representative) data to provide a signed consent form, which serves to confirm approval to collect, use and/or disclose personal information (including phone recordings by a third party). Consent will usually be required in writing, however verbal consent in certain circumstances (e.g. urgent service delivery, remote clients), may be accepted with efforts made to obtain written consent as soon as practicable.

What happens if we cannot collect personal information?

Wherever lawful and practical, individuals may interact with us anonymously or using a pseudonym. However, due to the nature of our services — including workplace rehabilitation, disability support, and health-related assessments — we are generally required by law or funding agreements to collect and use identifiable personal information. In these cases, anonymity or pseudonymity is not practicable.

More generally, if an individual does not wish to provide us with the personal information we ask for, we may not be able to:

- provide the requested services, either to the required standard or at all.
- provide information about the services that are wanted.
- engage the individual as an employee or contractor.
- maintain a relationship.
- improve our service to meet the needs of our valued clients.

- meet our funding, professional and legal obligations.
- respond to a person's complaint.

It may not be possible to tailor the content of websites to meet individual preferences, and as a result, a person's experience of the websites may not be as anticipated.

DISCLOSURE OF PERSONAL INFORMATION

To whom will we disclose personal information?

We only share personal information with stakeholders that we have consent to share information with, or with stakeholders that we are required to share information with by law.

Disclosure of information may be provided to stakeholders involved in the scope of services, such as:

- Government Agencies/Government Departments
- Employment Services Providers
- Treating practitioners
- Nominated support person/s.
- A legal entity
- Prospective employers
- Prospective training organisations
- Prospective equipment suppliers
- Community providers engaged for the purpose of services.

We only disclose personal information as set out in this privacy policy and any specific privacy collection notice relevant to a person's service or engagement with us or to third parties as authorised or required by law or a court/tribunal order. In all other circumstances, we will disclose personal information only with prior consent from the individual involved.

Do we disclose personal information to anyone outside Australia?

We do not disclose personal information to anyone outside Australia unless it is part of the service we provide. In certain circumstances, NDIS services (i.e. s speech pathology, psychology and occupational therapy for conducting assessments and online evaluations) may be provided from a health practitioner, outside Australia. In this instance we may disclose personal information overseas with consent. Further details can be found in the specific privacy collection notice relevant to each service.

We do use social media platforms such as Facebook and LinkedIn to facilitate our business activities and functions and post about services, employment opportunities and other information about our events and activities. If an individual

chooses to interact with us through these services, it is their responsibility to review and accept the privacy policy of that third party social media service prior to interacting with us.

PROTECTING PERSONAL INFORMATION

We are committed to 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 smart phones 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 measures for our website(s).
- ISO 27001: Information Security Management Systems certification

ACCESSING AND CORRECTING PERSONAL INFORMATION

An individual may request access to personal information that we hold about them. The process for requesting and obtaining access to personal information is as follows:

- Make a request for personal information in writing and address our Privacy Officer (details provided below). The request should specify if access is needed by photocopy, electronic copy, or visual inspection.
- Provide as much detail as possible regarding The Arriba Group business, department and / or person to whom personal details have been provided and when. This will help us to process the request more efficiently.
- We will endeavour to acknowledge the 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 the person know the anticipated time for a response to be provided.
- Requests for personal information will need to be verified with identity documentation 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, the person 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 a person's information is found to be incorrect, a correction or deletion may be requested.
- 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.

It is important to us that the personal information we hold is up to date. We will take reasonable steps to make sure that personal information is accurate, complete and up to date. If the information we have is not up to date or is inaccurate, a request for correction to personal information can be made by contacting our Privacy Officer. We will respond within 30 days and may charge a reasonable fee for access. If access or correction is denied, an explanation will be provided.

RETENTION OF PERSONAL INFORMATION

Subject to our retention requirements for health information outlined below, we will only keep personal information for as long as it is needed for any purpose for which it was collected, or otherwise if it is part of a Commonwealth record or is required to be retained under Australian law or by a court or tribunal. Personal information that is no longer needed or legally required will be de-identified or destroyed.

In accordance with the State-based health information protection laws, we are required to retain health information for seven (7) years after the last occasion on which we provided a health service to an individual, except where the information was collected while the individual was under 18 (in which case, we will keep the records until the individual has reached 25 years of age).

DATA BREACHES

If a data breach occurs, Arriba Group is committed to swift action and transparent communication. Immediate steps are taken to contain and assess the breach, ensuring that any risk to personal information is minimised. The affected individuals are notified as required by law, and detailed investigations are conducted to determine the cause and extent of the breach. Remedial actions are implemented to prevent recurrence, and the relevant regulatory authorities are informed in line with privacy legislation. Arriba Group prioritises accountability and strives to maintain the highest standards of data security and trust with all stakeholders.

ENQUIRIES & COMPLAINTS

We respect a person's right to complain if they think their privacy has been breached. For privacy questions, concerns, or complaints, please contact our Privacy Officer. We will respond promptly after receiving a complaint to discuss practical solutions.

We will aim to resolve the complaint in a timely and appropriate manner. If we fail to respond to a complaint within 28 days of receiving it in writing or if there is dissatisfaction with the response that is received, a complaint can be made to the applicable regulator, such as the Federal Privacy Commissioner (the OAIC) or the relevant State or Territory Privacy Commissioner or equivalent regulator. Contact details for our Privacy Officer are:

Privacy Officer
Arriba Group
Suite 15.04, level 15/680
George Street
Sydney NSW 2000
T 1300 762 989
privacy.officer@arribagroup.com.au

RELATED DOCUMENTS

- Notifiable Data and Privacy Breach Form
- Data Breach Response Policy & Procedure
- Artificial Intelligence AI Usage Policy
- Information Security Policy