PRIVACY POLICY

POLICY

Throughout this document The Arriba Group refers to the group operations of Livebig Pty Ltd, Rehab Management (Aust) Pty Ltd and Aimbig Employment.

The Arriba Group is guided by and complies with the requirements of the Privacy Act 1988 (including the Australian Privacy Principles and amendments to the Act). The Arriba Group is also guided by and specifically comply with the requirements and the Health Records and Information Privacy Act 2002 (NSW) and the Australian Privacy Principles.

The Arriba Group takes its obligations under the Privacy Act seriously and takes all reasonable steps in order to comply with the Act and protect the privacy of the personal information that we hold. Some of this information may be health related.

The Arriba Group will need to collect and record personal and/or sensitive information that is relevant to our client's current situation and the scope of services. This information assists to ensure the services delivered are based on their current situation and needs.

The personal information collected, is on behalf of our contracted obligations held with our customers, and is subject to restrictions imposed on its disclosure, collection and use by the Privacy Act 1988 (Cth) (Privacy Act).

The Arriba Group are obliged, in accordance with the terms of their funding agreements, to comply with the Privacy Act when collecting, using and disclosing the personal information of customers, clients and related stakeholders.
Personal information is collected for the provision of employment, disability and occupational rehabilitation services to:

- Determine eligibility or appropriateness in services;
- Tailor services to clients' needs;
- Evaluate and monitor outcomes, programs and services provided;
- Facilitate resolution of complaints made by stakeholders;
- Allow for inclusion of client personal details in communications developed by the Arriba Group applicable to the scope of services.

SCOPE

This Policy relates to the collection, use and disclosure of information for:

- Stakeholders involved in the scope of services delivered by the Arriba Group
- Employees or prospective employees of the Arriba Group
- Contractors of the Arriba Group.

PURPOSE

The purpose of this policy is to state the commitment of the Arriba Group to comply with relevant legislation relating to Privacy and to outline the methods adopted to comply with legislation.

COLLECTION OF INFORMATION

Personal and confidential **information** shall not be **collected** by The Arriba Group for inclusion in a record unless the **information** is **collected** for a purpose that is a lawful purpose directly related to a function or activity provided by our organisation and when the collection of the information is necessary for or directly related to that purpose.

Where it is reasonable and practicable to do so, personal information is collected directly from the individual. Collection may take place for a number of purposes, which includes information pertaining to the delivery of services or internally as part of an employee's employment with the Arriba Group.

Examples:

- For the purpose of providing occupational rehabilitation, therapy and assessment and/or employment services in accordance with contracted agreements, a referral and legislative requirements;
- When registration forms for a service are required;
- When a request is made for information in writing or verbally;
- During the recruitment and selection process and during the course of employment with the Arriba Group.

Sometimes personal information may be collected from other sources, e.g.

- An employer for the purpose of establishing and delivering services;
- An insurance agent for the purpose of delivering occupational rehabilitation services;
- A community services provider to support the engagement of services that fall within the scope of services delivered by the Arriba Group;
- A medical practitioner delivering services, or to determine an employee of the Arriba Group's fitness for work.
- NDIS related stakeholders (e.g. Planners) for Livebig services only.

For DES related services, personal information may be passed on to the following departments and their respective contracted service providers for the purpose of employment-related services. This includes:

- Department of Social Services
- Department of Human Services
- Department of Education and Training
- Department of Home Affairs
- Department of Jobs and Small Business
- Department of the Prime Minister and Cabinet.

Personal information may also be disclosed between DES Providers in the event a client's existing provider is unable to provide services and transferred to another Provider is required. Personal information may also be used by the Department of Social Services (the Department) (Aimbig clients only) or given to other parties where the client has agreed or it is required or authorised by or under an Australian law or a court/tribunal order.

In most cases the Arriba Group will require individuals to provide consent for collection, use or disclosure of personal information (including phone recordings by a third party). Consent will usually be required in writing, however verbal consent in certain circumstances will also be accepted and documented for record keeping purposes.

The Department's Privacy Policy contains more information about the way it will manage a client's personal information, including information about how the client may access their personal information held by the DES Provider and/or the Department and seek correction of such information. This Privacy Policy also contains information on how you can complain about a breach of privacy rights and how the Department will deal with such a complaint. Click here to obtain a copy of the Department's Privacy Policy or request a copy from the Department by email: at complaints@dss.gov.au.

USE AND DISCLOSURE

The Arriba Group collects personal information to enable it to conduct its business, including

- Determining an individual's requirements for appropriate services;
- Setting up and administering services;
- Identifying a person and protecting that person from unauthorised access to his/her personal information;
- Recruitment and selection processes.

Personal information may be used for purposes other than for which it was collected, namely,

- To prevent a serious threat to a person's health or life;
- As required or authorised by law;
- Where reasonably necessary for the enforcement of criminal or revenue law.

The Arriba Group may disclose personal information where consent has been given. Consent to the disclosure of personal information may be given explicitly, such as in writing or verbally, or may be implied from conduct. Disclosure of information may be provided to stakeholders involved in the scope of services, such as:

- Employer;
- Referring agent/department;
- Treating practitioners;
- Nominated support person/s;
- Nominated Union delegate;
- A legal entity;
- Prospective employers;
- Prospective training organisations;
- Prospective equipment suppliers;
- Community providers engaged for the purpose of services.

When is disclosure not appropriate?

The Arriba Group do not collect personal or sensitive information unless the information is reasonably necessary for, or directly related to, one or more of the functions or activities we have been requested to undertake as a part of our service delivery and operations.

The Arriba Group do not disclose personal information to a party outside or unrelated to the scope of services. Parties that may be eligible to personal or sensitive information can include a party contracted to the Arriba Organisations to provide administrative services or activities on our behalf, and whereby that party is bound by the same privacy rules. The Arriba Group do not disclose personal or sensitive information to overseas recipients unless required to by law or if these recipients are directly related to the scope of services.

The Arriba Group do not disclose records of personal and sensitive client information or company intellectual property to ex-employees.

The Arriba Group do not disclose records that have been obtained by a third party, even if related to the scope of services provided. For example, the Arriba Group is not able to disclose independent medical and allied health assessments of documents obtained from a third party. However, clients can request access to those records from the owner/creator of those records directly.

In accordance with the Health Records and Information Privacy Act 2001, if the individual chooses not to provide the Arriba Group with personal information pertaining to their health and authority to collect and disclose information, we may not be able to provide the full range of our services.

CHILDREN AND YOUNG PEOPLE:

The Privacy Act 1988 (Privacy Act) protects an individual's personal information regardless of their age. An individual under the age of 18 has the capacity to consent if they have the maturity to understand what is being proposed. This is assessed on a case-by-case basis. If the Arriba Group believe or are unsure of the person's ability to consent, then the consent from a parent or guardian might be sought.

PROVISION OF A TELEHEALTH SERVICE

Where appropriate, the Arriba group services may be provided by telephone or videoconferencing. Clients and customers responsible for setting up the technology needed so they can access telehealth services. The Arriba Group employee providing services can assist with this if required. The Arriba Group will be responsible for the cost of the call to the client and the cost associated with the platform used to conduct telehealth services.

To access telehealth services, client's will be instructed that they require a quiet, private space; an appropriate device, i.e. smartphone, laptop, iPad, computer, with a camera, microphone, and speakers; and a reliable internet connection.

The privacy of any form of communication via the internet is potentially vulnerable and limited by the security of the technology used. To support the security of personal information, Rehab Management uses *Lifesize Cloud technology* which is compliant with the Australian standards for online security and encryption.

The Arriba Group will ensure we obtain permission and approval before recording any material via telehealth or otherwise, including taking photographic images, video, or audio for the purpose of observation and assessment. Any recorded material will be kept private and confidential and will be destroyed once the Arriba Group has completed the assessment and formulated the relevant documentation required.

Limitations of Telehealth

A telehealth consultation may be subject to limitations such as an unstable network connection which may affect the quality of services. In addition, there may be some services for which telehealth is not appropriate or effective. The Arriba Group will consider and discuss with clients and customers the appropriateness of ongoing telehealth sessions.

DATA SECURITY

The Arriba Group will take all reasonable steps to protect the security of personal and sensitive information collected. This includes measures to protect electronic materials and materials stored and generated in hard copy.

T The Arriba Group store sensitive and confidential information developed on our security controlled database. This database enables the Arriba Group to lock access to various users, as deemed appropriate regarding the nature of information and purpose for which that information has been obtained.

The Arriba Group operate within a secure and encrypted network that cannot be accessed by external stakeholders. The Arriba Group further operates as a paperless office where possible. However, if confidential or sensitive information is in written format on paper, this information is discarded using a secure paper removal and destruction process once no longer required.

Where information cannot be destroyed and needs to be maintained, the Arriba Group archive documentation using a professional document management company location. Confidential and sensitive information can then be made available to individuals on request and in accordance with Privacy laws.

SURVEILLANCE-CCTV

Surveillance such as CCTV cameras will be installed in the workplace.
The purpose of the CCTV cameras is to ensure the safety and security of all employees as the Employer wants to take proactive action to ensure all employees are safe and feel safe in their working environment.
You may consult with the Employer regarding any concerns about surveillance. All cameras are visible and will not be placed in bathrooms or change rooms.
The surveillance may be conducted at any time and be subject to surveillance in accordance with the Privacy Act 1988.
Please note the Employer reserves the right to refer to any surveillance footage during a disciplinary meeting.

ACCESS AND CORRECTION

The individual may request access to any personal information directly relating to them that has been developed and held by the Arriba Group. Only information pertinent to that individual will be disclosed.

In most cases, a summary of personal information such as name, address, contact telephone numbers, reports developed by the Arriba Group and service delivery notes can be made available to the individual by making an application in writing to the Arriba Group.

If the individual is able to establish that the information is not accurate, complete and up-to-date, the Arriba Group will take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

Should it be deemed necessary to refuse access or correction to an individual's information, the Arriba Group will provide reasons for denial of access or a refusal to correct personal information. The Arriba Group may refuse an individual access to personal information in a number of circumstances such as where the information may be related to existing or anticipated legal proceedings, where access to the information could result in potential harm to the individual's physical or mental wellbeing, where denying access is required or authorised by law, or where the request for access is regarded as frivolous or vexatious.

The Arriba Group is required by law to retain personal information for a period of time after an individual has ceased any relationship with us. After the required time has passed, the Arriba Group attend to the secure destruction or deletion of personal information related to interested parties where disclosure was previously authorised for collection and disclosure.

For information which has been archived, a fee may be charged to cover the cost of retrieval and the supply of this information. All requests for access to personal information will be handled as quickly as possible and the Arriba Group shall endeavor to process any request for access within 30 days of having received the request. Some requests for access may take longer than 30 days to process depending upon the nature of the personal information being sought.

BREACHES IN CONFIDENTIALITY

A breach in confidentiality relates to a Notifiable Data Breach that is likely to cause serious harm to an individual or individuals impacted by that privacy breach following unauthorised access, disclosure and/or loss of personal information.

Where a breach in confidentiality has been identified, the Manager will undertake the following activities ASAP:

- Notify the impacted party/parties immediately of any threatened or actual privacy events; and
- Consider and action all reasonable requests and directions from the interested parties.
- Where notifiable data breaches have occurred, the Manager will assess the impact on interested parties and in negotiation with the related parties, determine if the breach constitutes a requirement to notify the Office of the Australian Information Commission (OAIC). Notifying the OAIC will be completed by the QA & Compliance team.
- Where the Arriba Group has informed the OAIC, we will cooperate and notify impacted parties of the breach in relation to the assessment and reporting of a breach to the OAIC and notification to impacted customers.

COMPLAINTS

If the individual requires additional information or has any complaints about the privacy practices of the Arriba Group, individuals may contact the Director/s of The Arriba Group to lodge a formal complaint. Should the individual not be satisfied with the outcome of the internal complaint process, the individual may contact the following external entities:

Office of the Australian Information Commissioner
GPO Box 5218 SYDNEY NSW 2001 | www.oaic.gov.au

Privacy Commissioner

GPO Box 5218 Sydney NSW 2001 | Privacy Hotline: 1300 363 992 | Telephone: (02) 9284 9800 | Fax: (02) 9284 9666

DES Specific:

The Complaints Resolution and Referral Service (CRRS) on 1800 880 052 is available for you to discuss any concerns you may have about your Disability Employment Services (DES) provider. Phone: 1800 880 052 (free call)

EMPLOYEES

The Arriba Group respect the individual rights of its employees and consequently manages records it keeps in relation to employees in a careful and responsible manner. The Arriba Group are required to keep personal records for seven years from the date an entry is changed or from termination of an employee's employment, depending on what happens first.

Access by an employee to his/her own personnel file is generally permitted. An employee may have access to:

- His or her time and wages records, including overtime (if applicable) and remuneration;
- His or her records of leave, including leave taken and available entitlement;
- His or her records of superannuation contributions; and
- Workers compensation records if an employee has had an accident.

Employees should lodge a request with sufficient notice to allow documents to be retrieved to the Head of People and Culture and their Direct Manager.

Access by an employee to records of other employees is generally not permitted. If an employee believes that a special case exists and the other employees involved do not object then the manager may permit such access. The Managing Director will make the final decision regarding one employee having access to another employee's personnel file.

An employee may request an interview with their employer, the Arriba Group, or a representative of the employer at any time during working hours to discuss a record which has been made or is to be made by the Arriba Group.

When a third party, e.g. a bank or real estate agent requests information about an employee, that employee will be contacted and his/her permission will be required, in writing, before any information is released.

CONTRACTORS

All staff should be aware that personal information about contractors is not an 'employee record' and due care must be exercised in handling such information within the law.

UNSUCCESSFUL JOB APPLICANTS

In preserving the privacy of unsuccessful candidates by destroying records, it is difficult to prove a fair process. Consequently the practice outlined below is to be generally followed as part of the recruitment process. Applications and associated documentation will be held for a reasonable period of time after a position is filled, unless the candidate requests the information be filed in the event of other positions arising with the company. If any dispute arises, both parties will have relevant evidence to refer to. Candidates have the right to withdraw or ask for special treatment of their personal information if they do not agree with this stated practice.

PROCEDURE

SUSPECTED OR ACTUAL DATA BREACH OCCURS

IMMEDIATE RESPONSE ONCE IDENTIFIED?

1. *Immediately* notify your direct Manager. If a direct Manager is not available, notify either:
    a) QA & Compliance via the 'Quality' email group
    b) Client Relationship Manager if applicable
2. Record and advise notified Manager of the data breach details. Including: time and date the suspected breach was discovered, the type of personal information involved, the cause and extent of the breach, and the context of the affected information and the breach.

RECORDING THE DATA BREACH

The Notified Manager must complete the following actions:

- Complete the Notifiable Data and Privacy Breach Form within *4 hours* of being notified of the breach or suspected breach

RESPONSE ACTION BY MANAGER NOTIFIED

Email the Notifiable Data and Privacy Breach Form to the following Data Breach Response Team (DBRT) within the 4hr timeframe:

- Direct Manager (if they were not the initial Manager contacted)
- Head of QA & Compliance via 'Quality email group

SEVERITY ESCALATION

The DBRT will determine the need to escalate the data breach to additional Managers.

Where a data breach poses minimal risk to the organisation and those impacted by the data breach, the DBRT will delegate and communicate instructions for the most appropriate Manager to manage the data breach at a local level and ensure resolution of the issue within 1-business day.