

## POLICY STATEMENT

As *arbias* staff have access to clients' personal information, it is essential that they follow practices which protect clients' right to confidentiality and privacy.

## SCOPE

This policy applies to all *arbias* Board of Directors, Executive Management, staff, volunteers and students.

## PURPOSE

The purpose of this policy is to establish standards of confidentiality and privacy in work that *arbias* undertakes, including all information that is collected, stored and shared internally and externally. Staff members are required, during their employment and all time after cessation of the employment relationship, to

- Maintain the utmost confidentiality in relation to client and *arbias* business; and
- To assign all copyright in any material produced in the course of employment with *arbias*

## PROCEDURES

The following procedures are to be implemented to ensure that *arbias* meets its policy objective of ensuring that all people we support have the same level of confidentiality and privacy as is expected.

*arbias* will:

1. Only collect information about the person that is directly relevant to effective service delivery and the organisation's duty of care responsibilities.
2. Seek the written consent of the person and/or legal guardian (if applicable) prior to obtaining information from any other source.
3. Seek the written consent of the person and/or legal guardian (if applicable) prior to releasing or disclosing information to any other source. In the event there is doubt about the individual's ability to provide informed consent *arbias* will seek advice from the Neuropsychologist and the Neuropsychological report.
4. Staff cannot release data to any external person or body without express consent from the CEO. Data cannot be stored on any external device other than the *arbias*' SharePoint system.
5. Seek verbal consent from the person and/or legal guardian (if applicable) only when written consent is unable to be obtained.
6. Ensure that personal information is stored securely and is not left on view to unauthorised *arbias* staff or the general public.
7. Ensure that only those *arbias* staff that need access to the above information will be granted access.
8. Advise the person of the nature of the personal information that is held by *arbias* about the person.
9. Advise the person and/or legal guardian (if applicable) of their right to request to view the information that *arbias* keeps in respect of the client.
10. Ensure that personal information about the person is only held by *arbias* as long as it remains relevant to the delivery of effective services and the organisation's duty of care obligations and as per legislative requirements.
11. Promptly investigate, remedy and document any grievance regarding confidentiality and privacy utilising the Managing Feedback and Complaints Policy.

**Consent**

In the instance where a person or agency refers someone to our services, arbias must obtain a signed consent form. The consent form must be dated and is valid for 12 months. Consent can be withdrawn at any time.

**Confidentiality of Client Information**

arbias' policy regarding confidentiality is embodied in the following principles:

The decision to collect and disclose information is based on the best interests of the client.

- Only relevant information is collected.
- Advice is given to clients about the purpose of information collection and conditions regarding release before these actions occur.
- The client has control over details recorded.
- There must be no unreasonable personal intrusion when collecting information.

Files must be stored securely.

- Only people who "need to know" can have access to information.
- Informed consent from the client is required to release information in most circumstances.
- All clients have the right to access their own personal information.

All arbias staff will follow the Confidentiality and Privacy Policy when carrying out their duties.

**Collecting Information**

Where a staff member receives information from a client, the staff member should be mindful of the requirements of privacy legislation with respect to that information and should maintain confidentiality of the information during their employment with arbias and after cessation of the employment relationship. arbias Privacy Policy should be referred to in this regard.

When collecting information arbias staff must advise the client of the following:

- Why the information is being collected.
- That all information will be kept in a file.
- That the information given by the client, or any other source, may, under certain circumstances, be released without the client's or guardian's consent. For example, information may be given to the Guardianship and Administration Board, police, courts or Departmental program areas such as Protective Services. This information must be disclosed if the file has been subpoenaed because it may contain material which relates to abuse, neglect, exploitation, victimisation or to an alleged criminal offence. Staff must explain to the client or guardian why disclosure of information is necessary in these cases.
- That staff may contact other sources to collect information about the client and, where possible, ask the client to sign a release of information form.
- That the client can access their own file.

arbias staff must recognise and respect the client's role in controlling what information is revealed and recorded.

Only information related to meeting the client's needs should be collected and recorded. That is, information must be necessary for effective service delivery to that client.

Collecting information must not intrude unreasonably on the client's personal affairs.

**Collection Statement**

arbias collects personal information for the following purposes:

- Conducting recruitment and appointment of staff;
- Conducting employment relationships with staff;
- Monitoring the services provided to *arbias* clients;
- Monitoring use of our website;
- Processing payments;
- Promoting the work of *arbias*;
- Liaising with other agencies in the course of conducting the work of *arbias*;
- Providing services to our clients; and
- To comply with our legal obligations.

**Personal Information Collected**

*arbias* may collect, use, and hold the following personal information:

- Your name
- Personal History
- Business Address
- E Mail Address
- Telephone / Fax Numbers
- Occupation
- Medical History
- Family History and Contact Details

This personal information can contain sensitive information such as health information and your membership of a professional or trade association. Arbias will not collect sensitive information about an individual, such as ethnicity or criminal record, unless the information is needed to provide the service in accordance with the individual's personal plan, to ensure our duty of care and or to meet our legal requirements.

When you visit our website to read or download information, our internet service provider collects the following information:

- Your server address
- Your domain name
- The date and time of your visit to our site
- The pages viewed
- The information downloaded.

Our website does not use "cookies".

**The way information is collected**

*arbias* will not collect personal information unless the information is necessary to enable us to undertake our activities.

We will endeavour to collect personal information about you primarily from you. However, in some circumstances, we collect personal information about you from a third party. For example, we may collect personal information from an organisation that you work for.

If we collect personal information about you from a third party, we will take reasonable steps to contact you and ensure that you are aware of the purposes for which we are collecting your personal information and the organisations to which we might disclose your personal information.

At the point of initial enquiry the individual will be provided with a unique identifier within the records held by Intake and Response and or the Assessment unit. Ensuring anonymity will be afforded to the extent that arbias can depending on the level of access to our services required by the individual.

***If personal information is not disclosed***

You are not obliged to give us your personal information. However, if you choose not to provide arbias with personal details we may not be able to provide you with a service, communicate with you effectively, process your payment in a particular way or process your application for employment.

***Security, disclosure and transfer of personal information***

We will take all reasonable steps to protect the security of the personal information of yours that we hold. This includes appropriate measures to protect electronic materials and materials stored and generated in hard copy.

arbias will only usually disclose this information to:

- Our accountants and auditors
- Our IT managers
- Our legal representative
- Our clients, where we have collected that information in the course of providing services to them
- GP and Health Specialists
- Welfare Providers
- Legal Personnel

arbias takes contractual measures to protect the personal information we provide to organisations and people that provide services to us.

arbias does not generally transfer any information overseas.

***Trans-border Data Flows***

arbias will only transfer personal information about an individual to arbias staff or contractors in another state where those staff or contractors will be contributing to or delivery supports to the individual.

***Disclosing Information With Consent***

In most circumstances, the client's consent must be sought when the release of information is required. The client's consent, or refusal to consent, to the disclosure of information must be noted in the client's file. If the client does not have the capacity to make an informed decision regarding

the disclosure of information, staff must consult the client's legal guardian. If the client does not have a legal guardian, an application must be made to VCAT for a guardian to be appointed.

### ***Disclosing Information Without Consent***

Consent is not required if information is:

- Necessary to prevent or lessen a serious threat to the life or health of the client.
- Subject to a subpoena.
- Reasonably necessary for the enforcement of the law, or for the protection of public money.
- Used for the purpose for which it is obtained. For example, a record of the client's medical issues may be required by the doctor managing the client's treatment.

Release of information must be on a "need to know" basis, rather than a "want to know" basis. Staff must never discuss personal client information to anyone who does not need to know, either at work or outside the workplace. For example, if a psychologist is advising staff on the management of a client's behaviour, they would not necessarily need to know about the client's financial situation.

### **Access and Storage**

Personal information must be stored securely. Staff must lock away clients' files when not in use. Documents cannot be removed from client files without permission of a senior manager.

- Printed items should be collected immediately from printers and faxes.
- Client files must not be left unattended on the photocopier or any other part of the building.
- When referring to a client in an email, only first name or initials should be used.
- Staff access the electronic records via a personal login codes
- Access to electronic files are limited via permissions to the respective program areas
- Staff cannot view records that are not applicable to their work.
- The system identifies the respective staff member when accessing to view electronic files.
- If a staff member has any doubt at any time with respect to confidentiality and privacy in relation to information received from a client, the staff member should discuss the matter with the Chief Executive Officer.

Confidentiality practices relate specifically to clients, however personal information about a client's family or guardian must also be dealt with in a confidential manner.

### ***Individuals accessing their own personal information***

You may seek access to the personal information pertaining to you that has been collected by *arbias*.

At all times the conduct under this Policy will be governed by the following principles:

- All requests for access will be treated seriously
- All requests will be dealt with promptly
- All requests will be dealt with in a confidential manner
- Your request to access your personal information will not effect your existing obligations or affect any arrangements between you and *arbias*.

### ***How do I request access to information?***

- Your request for access to personal information must be made in writing.

- You must provide proof of your identify when requesting access to personal information. This is necessary to ensure that information is provided only to the correct individuals and that the privacy of others is not undermined.
- You may request access to personal information by writing to the Chief Executive Officer, *arbias* Ltd PO Box 5002, Brunswick North 3056.

### ***Form of Access***

- If *arbias* agrees to provide you with access, *arbias* will allow you to inspect, take notes of or receive copies or print outs of the personal information that *arbias* holds about you.
- If an individual establishes that the information is not accurate, complete and up to date, *arbias* will correct the information within ten working days and provided substantiation to the individual that this has been undertaken.

### ***When will Access be denied?***

Access will be denied if:

- The request does not relate to the organisational or personal information of the person making the request;
- Providing access would create an unreasonable impact on the privacy of others;
- The request is frivolous and vexatious;
- The request relates to existing or anticipated legal proceedings between *arbias* and the person making the request;
- Providing access would prejudice negotiations with the individual making the request;
- Access would be unlawful;
- Denial of access is authorised or required by law;
- Access would prejudice law enforcement activities;
- Access discloses a commercially sensitive decision making process or information;
- Providing access would pose a serious and imminent threat to life or health of a person; or
- Any other reason that is provided for in the National Privacy Principles (NPPs) set out under the *Privacy Act 1998* (Commonwealth).

Where possible, *arbias* will favour providing access. It may do so by providing access to the appropriate parts of the record or by using an appropriate intermediary. Where there is a dispute about the right or forms of access these will be dealt with in accordance with *arbias*' Grievance Policy.

### ***Time for providing access***

We will take all reasonable steps to provide access within a reasonable time of your request. In cases where the request is not complicated or does not require access to a large volume of information, we will provide information more quickly.

### ***Costs and charges***

*arbias* may impose the following charges inclusive of GST:

- Photocopying \$2 per page
- Delivery cost of information stored off-site – where information is stored off-site, the cost of obtaining access to the information - \$30 per hour
- Access to electronic databases \$30 per hour
- Postage Costs

**Confidentiality of arbias Information**

During the currency of their employment with arbias and at all times after the cessation of the employment relationship, arbias staff members (or former staff members), must keep confidential:

- Any and all marketing information, for example but not limited to client or related organisation lists, financial information and business plans;
- Any and all documents or information marked as confidential and any information received or developed by the staff member in the course of his or her employment that is not publicly available and relates to processes, equipment and techniques used by *arbias* in the course of its business.
- Staff members must not at any time share confidential information with any other person, except with the written authority of the Executive Officer.
- Staff members (or former staff members) must not use confidential information for any purpose other than to benefit *arbias*.
- *arbias* staff members must return any or all confidential information to *arbias* if requested to do so.
- Staff members must not appropriate, copy, memorise or in any way reproduce any confidential information obtained in the course of employment with *arbias*.

**PRIVACY STATEMENT**

*arbias* is committed to acting in accordance with its obligations under state and federal privacy legislation, including the *Privacy Act 1988* (Cth), the *Health Records Act 2001* (Vic), the *Information Privacy Act 2000* (Vic) and the *Health Records and Information Privacy Act 2002* (NSW)

*arbias* takes all reasonable steps to comply with the relevant legislation and protect the privacy of any person's personal information that is held by *arbias*. This policy outlines *arbias* compliance strategies.

**HOW PRIVACY COMPLAINTS ARE HANDLED**

*arbias* sees the importance of privacy to the organisation, its customers and other stakeholders.

As such, *arbias* is committed to protecting the privacy of the personal information that we hold. This is part of our organizations':

- Legal obligations under the *Privacy Act 1988*
- Ethical and business obligations
- Service to you

*arbias* places high priority on effectively dealing with any complaints about privacy that you may have.

**Overriding principles**

At all times conduct under this policy will be governed by the following principles (as per the Managing Feedback and Complaints policy):

- All complaints will be treated seriously
- All complaints will be dealt with promptly.
- The individual will receive acknowledgement of the complaint within three working
- *arbias* will make all reasonable attempts to resolve the complaint within ten working days. The individual will be advised if there is a likelihood that the resolution will take longer than ten days.

- All complaints will be dealt with in a confidential manner
- Any privacy complaint will not affect your existing obligations or the commercial arrangements that exist between this organisation and you.
- The individual will be advised of their right to access an advocate. If requested arbias will provide a list of Advocates.

***What is a privacy complaint?***

A privacy complaint relates to any concern or dispute that you have with our privacy practices as it relates to your personal information. This could include matters such as:

- How information is collected
- How information is stored
- How this information is used or disclosed
- How access is provided
- How accurate the information that we hold is
- All staff will record every complaint received on a register.
- The CEO will review the register on a monthly basis

***What do I do if I have a complaint about privacy practices?***

arbias resolves grievances at the local level if possible. If you have a complaint about privacy please contact the CEO or delegate. All complaints will be logged on a the Complaints Register (on Sharepoint). You may complain orally or in writing to:

Chief Executive Officer, **arbias** Ltd, PO Box 5002, Brunswick 3056

Usually your contact with **arbias** will be the appropriate person to discuss or resolve your complaint. However, if your privacy complaint is not resolved the matter will then be referred to an external and independent mediator. See the arbias Managing Feedback and Complaints Policy for more details.

**PERFORMANCE STANDARDS**

The following performance standards must be met to ensure that the procedures are implemented effectively:

1. All service users and employees have been provided with a copy of the organisation's policy on Confidentiality and Privacy; and any grievances are addressed in accordance with the principles outlined in this policy as well as the Managing Feedback and Complaints Policy.
2. The person has been informed why the information sought is required by the organisation; and the consent forms have been completed by the person supported by arbias prior to information being collected or provided to/from other sources (note photographic, video or other identifying images will not be displayed or aired publicly without the written prior permission of the person).
3. Client files are stored in lockable filing cabinets in a non-public place in the office with no identifying information on obvious display; and files are returned to their proper location as soon as they are no longer required and shredded / removed electronically from the server after a period of no less than seven years.



## **Relevant Links:**

### **STANDARDS:**

*Department of Health and Human Services Standards (Victoria)*

Standard 1: Empowerment

*Disability Service Standards (NSW)*

Standard 1: Rights

Standard 4: Feedback and Complaints

### **LEGISLATION**

Disability Act 2006 (Vic)

Disability Inclusion Act 2014 (NSW)

Privacy Act 1988 (Commonwealth)

Information Privacy Act 2000 (Vic)

Health Records and Information Privacy Act 2002 (NSW)

Health Records Act 2001 (Vic)

### **Related Policies & Procedures:**

Policy - Advocacy

Policy – Managing Feedback and Complaints