PRIVACY AND CONFIDENTIALITY OF INFORMATION POLICY

POLICY STATEMENT

This policy has been designed with recognition that Open Minds must adhere to the National Privacy Principles and the *Privacy Amendment (Private Sector) Act 2000.* These principles and the privacy legislation set standards that must be met when collecting, holding, using and the disclosure of private or sensitive information.

PURPOSE

2.1. The purpose of this policy is to set an expected level of personal and professional behaviour for all workers with Open Minds in the handling and transmission of sensitive (private) information. This policy shall be implemented to ensure that this objective is upheld.

2.2. This policy outlines Open Minds process for capturing and managing personal information.

SCOPE

3.1. This Policy applies to Open Minds' directors, officers, workers, clients, volunteers, interns or persons undertaking work experience, and independent contractors and consultants engaged in providing paid or in-kind services to or on behalf of Open Minds.

DEFINITIONS

4.1. Commonly defined terms and acronyms are located in Open Minds' Policy Framework Policy.

4.2. Reference to specific employment positions are linked to the OM Organisational Structure available on Open Minds Intranet.

4.3. The following definitions apply for the purpose of this Policy:

'Worker' – For the purpose of this policy, "worker" may include any of the following:

a) an employee; or

b) a contractor or subcontractor or an employee of a contractor or subcontractor; or

c) an employee of a labour hire company who has been assigned to work at Open Minds

d) an apprentice or trainee; or

e) a student gaining work experience; or

f) a volunteer.

'Client' – refers to a person accessing any Open Minds service. This includes past clients, persons making enquiries and/or persons who may receive services in the future.

'Privacy' - refers to workers and clients personally - that is, about his or her body, support needs, family and friends, relationships, lifestyle, home, workplace, belongings, and finances.

'Confidentiality' – refers to information (written, spoken and observed) about the workers and clients - that is about his or her conversations, file, reports, programs, activities.

'Information' – refers to information or an opinion about an identified individual, or an individual that is reasonably identifiable:

a) Whether the information or opinion is true or not; and

b) Whether the information or opinion is recorded in a material form or not.

'Personal information' – includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.

For example, personal information may include:

a) an individual's name, signature, address, phone number or date of birth

b) sensitive information

c) credit information

d) employee record information

e) photographs

f) internet protocol (IP) addresses

g) voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique)

h) location information from a mobile device (because it can reveal user activity patterns and habits)

'Sensitive information' - is personal information that includes information or an opinion about an individual's:

a) racial or ethnic origin

b) political opinions or associations

c) religious or philosophical beliefs

d) trade union membership or associations

e) sexual orientation or practices

f) criminal record

g) health or genetic information

h) some aspects of biometric information

Generally, sensitive information has a higher level of privacy protection than other personal information.

PRINCIPLES

The following principles apply when interpreting and applying the Policy Requirements set out in Section 6 below:

5.1. The following principles apply when interpreting and applying the Policy Requirements set out in Section 6 below:

5.2. Open Minds is committed to ensuring the privacy and confidentiality of personal information is upheld in accordance with the *Privacy Act 1988.*

5.3. We do this by ensuring procedures and practices comply with the 10 National Privacy Principles described in the *Privacy Amendment (Private Sector) Act 2000*.

5.4. Accordingly, as a minimum, the following statements are observed in the creation or implementation of any procedures or practices at Open Minds:

a. Open Minds only collects information relevant to the services it provides and only collects information in a lawful and fair way and by means that are not unreasonably intrusive

b. Open Minds informs its stakeholders of the need to gather information, their right to access their own records and their right to request inaccuracies to be corrected if they are found to exist

c. Open Minds seeks consent prior to disclosure of information for purposes other than those identified within this policy

d. Open Minds does all it can to keep stakeholders personal information up to date, accurate and complete

e. Appropriate access restrictions are applied to electronic information across the organisation. Paper-based information is kept secure at all times

f. Any identifiers used by Open Minds are unique forms of identification that are not derived from any other personal identifiers such as Medicare or Tax File Numbers

6. COLLECTION OF INFORMATION

6.1. Information will only be collected where the information is necessary for one or more of Open Minds functions or activities.

6.2. Personal information will only be collected by lawful and fair means not in any unreasonably intrusive way

6.3. Open Minds will take reasonable steps to inform individuals about the use of their personal information. Individuals will be aware of:

a) Open Minds and their contact information

b) How individuals can access their personal information

c) Purpose for which the information is collected

d) Types of other organisations the individuals personal information may be disclosed

e) Any law that requires the particular information to be collected

f) Consequences (if any) for the individual if all or part of the information is not provided

g) No information is collected about an individual without their consent

7. USE AND DISCLOSURE OF INFORMATION

7.1. No information is disclosed about an individual without their written consent except:

a. Non-identifying data required by funding bodies and by government departments for planning purposes

b. Where disclosure is required or authorised by law (such as court subpoena or staff testifying under oath)

c. Where it is reasonable to believe the disclosure is necessary to prevent or lessen serious threat to the life or health of the client or another person

d. Where it is reasonable to believe the disclosure is necessary for the enforcement of the criminal law or for a law imposing a fine or for the protection of public revenue

e. Within the natural course of business activities including the use of staff names and their position within the organisation within press releases, internal and external newsletters, organisational website or other promotional materials

7.2. Where information is disclosed, it is only to be used for the purpose for which it was disclosed

7.3. Open Minds workers who have access to information about any other individual, whether in hard copy, electronic or knowledge, must not disclose or release this knowledge/information unless it is essential for business activities with written approval

7.4. Prior to granting access to any personal client information all workers will be required to sign the Worker Confidentiality Agreement

7.5. Information about Open Minds business functions or operations such as worker pay rates, specific client groups or operational information held in confidence must not be disclosed without the prior written consent of the Chief Executive Officer

8. CLIENT FILE REQUEST

8.1. Clients have the right to request or view their file at any time

8.2. All requests must be in writing and forwarded to the General Manager of the associated program for actioning

8.3. The General Manager will consider all requests made by clients and should there be no eminent health risk to the client, information will be provided

8.4. Should the General Manager identify a risk to clients mental health or other physical injuries that may arise following the disclosure of information from a client's file to a client, this particular information will be withheld

9. INFORMATION SECURITY

9.1. All information relating to stakeholders and documents whether written, electronic, spoken or observed is to be treated as private and confidential

9.2. Open Minds and its workers must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

9.3. Open Minds will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

9.4. All 'hard copy' confidential information relating to stakeholders must be stored securely.

9.5. 'Electronic information' is to be stored on a secured network with security permissions applied to allow access to persons with authority to access the particular content..

9.6. Open Minds information, communication and technology practices are maintained to keep up with emerging technologies, changes in business practices, threats to security and aligned to privacy legislation. Refer to Information Management Policy.

10. ACCESS AND CORRECTION

10.1. All stakeholders must be provided with access to their personal information upon request, except to the extent that:

i. In the case of personal information other than health information "providing access would pose a serious and imminent threat to the life or health of any individual"

ii. In the case of health information "providing access would pose a serious threat to the life or health of any individual"

iii. Providing access would have an unreasonable impact upon the privacy of other individuals

iv. The request for access is frivolous or vexatious

v. Information relates to existing or anticipated legal proceedings between Open Minds and the individual, and the information would not be accessible by the process of discovery in those proceedings

vi. Providing access would reveal the intentions of Open Minds in relation to negotiations with the individual in such a way as to prejudice those negotiations

vii. Providing access would be unlawful

viii. Denying access is required or authorised by or under law

ix. The prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of law imposing a penalty or sanction or breaches of a prescribed law

x. Providing access would be likely to prejudice

1. The prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of law imposing a penalty or sanction or breaches of a prescribed law
2. the enforcement of laws relating to the confiscation of the proceeds of crime
3. the protection of the public revenue
4. the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct
5. the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its order

xi. an enforcement body performing a lawful security function asks Open Minds not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia

xii. If Open Minds holds personal information about an individual and the individual is able to establish the information is not accurate, complete and up-to-date, Open Minds must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

xiii. Open Minds must provide reasons for denial of access or a refusal to correct personal information

11. IDENTIFIERS

11.1. Open Minds must not adopt associated identity of an agency, agent, State or Commonwealth department, who has referred an individual to our services as a contracted service provider.

12. ANONYMITY

12.1. Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with Open Minds.

13. TRANS BORDER DATA FLOW

13.1. Only the CEO of Open Minds may consider the transfer of personal information and only following receipt of individuals consent, across political boundaries, such as between states or countries.

14. SENSITIVE INFORMATION

14.1. Open Minds will not collect sensitive information about an individual unless:

a) The individual provides consent

b) The collection is required by law

c) The collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual where the individual whom the information concerns:

I. Is physically or legally incapable of giving consent to the collection

II. Physically cannot communicate consent to the collection

d) If the information is collected in the course of the activities of Open Minds the following conditions are satisfied:

I. The information relates solely to the individuals who have regular contact with it in connection with its activities

II. At or before the time of collecting the information, Open Minds undertakes to the individual whom the information concerns that they will not disclose the information without the individuals consent

e) The collection is necessary for the establishment, exercise or defence of a legal or equitable claim

14.2. Open Minds will collect health information about individuals if:

a) the information is necessary to provide a health service to the individual

b) the information is collected

c) required or authorised by or under law

d) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind Open Minds

ROLES AND RESPONSIBILITIES

POSITION	ROLE	RESPONSIBILITY
BOARD OR DELEGATE	Approve	Authorised to approve this Policy and any subsequent amendments to this Policy
CEO OR DELEGATE (ROLE SPECIFIC)	Owner	Accountable and responsible to: - ensure that this Policy is implemented and communicated; - issue procedures or documents to support the operation of this Policy; - receive and consider suggested improvements - ensure this policy and related documents are reviewed within required timeframes or earlier as required.
CEO OR DELEGATE	Review	Accountable and responsible to ensure this policy is reviewed as per this Policy or as required.

OPEN MINDS STAFF (AS PER SCOPE)	Implement	Responsible to: - read, understand and implement policy; and - suggest improvements as appropriate.

RELATED LEGISLATION AND STANDARDS

LEGISLATION AND/OR REGULATIONS
Privacy Act 1998
Privacy Amendment (Private Sector) Act 2000

COMPLIANCE AND REPORTING MEASURES

A report on all material breaches or non-compliances will be reported on quarterly basis to Board.

KEY RELATED DOCUMENTS

DOC TYPE OR ID	DESCRIPTION / NAME
TBA	Staff Personal Details Record
TBA	Request for Release of Personal Information
TBA	Worker Confidentiality Agreement
TBA	Information Management Policy
TBA	Data Management Strategy

POLICY REVIEW

This Policy should be reviewed, at a minimum, every three years, or updated more regularly where circumstances require.