Privacy & Confidentiality Policy Manual

29 South Corporate Drive, Rowville Vic 3178

ABN: 30 006 520 314

Version: 2

Approval Date: 1/08/2019

Review Date: 1/08/2022

Privacy and Confidentiality

PURPOSE AND SCOPE

OAPL to manage and ensure that the rights of the participants remain private and personal information if only used for the purpose for which it is collected.

This policy applies to all employees.

POLICY

OAPL is committed to protecting and upholding the right to privacy of participants, staff and management.

OAPL is committed to protecting and upholding the rights of our participants to privacy in the way we collect, store and use information about them, their needs and the services provided to them.

OAPL requires employees and management to be consistent and careful in the way they manage what is written and said about individuals and how they decide who can see or hear this information.

OAPL is subject to NDIS (Quality and Safeguards) Commission. The organisation will follow the guidelines of the Australian Privacy Principles in its information management practices.

OAPL will ensure that each participant / advocate / parent understands and agrees to what personal information will be collected and why, including recorded material in audio and/or visual format.

OAPL will advise each participant / advocate / parent of confidentiality policies using language and terms that the participant is most likely to understand.

OAPL will ensure that:

- It meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of participants and organisational personnel.

- Clients/participants are provided with information about their rights regarding privacy and confidentiality.
- All staff, management and volunteers understand what is required in meeting these obligations.

This policy conforms to the *Federal Privacy Act (1988)* and *the Australian Privacy Principles* which govern the collection, use and storage of personal information.

This policy will apply to all records, whether hard copy or electronic, containing personal information about individuals, and to interviews or discussions of a sensitive personal nature.

PROCEDURES

Dealing with personal information

In dealing with personal information, OAPL staff will:

- Ensure privacy for clients/participants, staff, or management when they are being interviewed or discussing matters of a personal or sensitive nature
- Only collect and store personal information that is necessary for the functioning of the organisation and its activities
- Use fair and lawful ways to collect personal information
- Collect personal information only by consent from an individual
- Ensure that people know what sort of personal information is held, what purposes it is held it for and how it is collected, used, disclosed and who will have access to it
- Ensure that personal information collected or disclosed is accurate, complete and up-to-date, and provide access to any individual to review information or correct wrong information about themselves
- Take reasonable steps to protect all personal information from misuse and loss and from unauthorised access, modification or disclosure
- Destroy or permanently de-identify personal information no longer needed and/or after legal requirements for retaining documents have expired.

Client/Participant Records

Client/Participant clinical records will be confidential to staff directly engaged in delivery of service to the participant. All information gathered is stored in in a secure office with out of hours security monitoring.

Staff can only access participant files whilst at work and during work hours. Some quotation- and assessment-specific participant data is backed up to cloud storage in case of theft or natural disaster. Digitally stored information is protected by password.

Responsibilities for managing privacy

- All staff are responsible for the management of personal information to which they have access, and in the conduct of research, consultation or advocacy work.
- Management is responsible for content in OAPL publications, communications and website and must ensure the following:
    - Appropriate consent is obtained for the inclusion of any personal information about any individual including OAPL personnel (Consent policy)
    - Information being provided by other agencies or external individuals conforms to privacy principles
- Management are responsible for safeguarding personal information relating to OAPL staff.
- Management will be responsible for:
    - Ensuring that all staff are familiar with the Privacy Policy and administrative procedures for handling personal information
    - Ensuring that clients/participants and other relevant individuals are provided with information about their rights regarding privacy
    - Handling any queries or complaint about a privacy issue

Privacy information for NDIS participants

Participants will be told what information is being collected, how their privacy will be protected and their rights in relation to this information within their service agreement and through our 'Your Privacy and Confidentiality' pamphlet.

To ensure privacy for participants or staff when discussing sensitive or personal matters, the organisation will:

- Only collect personal information which is necessary;
- Which is given voluntarily; and
- Which will be stored securely

OAPL will not disclose such personal information to a third party:

- Without the individual's consent; or
- Unless that disclosure is required or authorised by or under law

Sharing information without consent

If required or authorized by law OAPL may have a duty of care to share your information with authorities. In this instance, the Information Sharing Guidelines are followed, as outlined in appendix 3 within this policy.

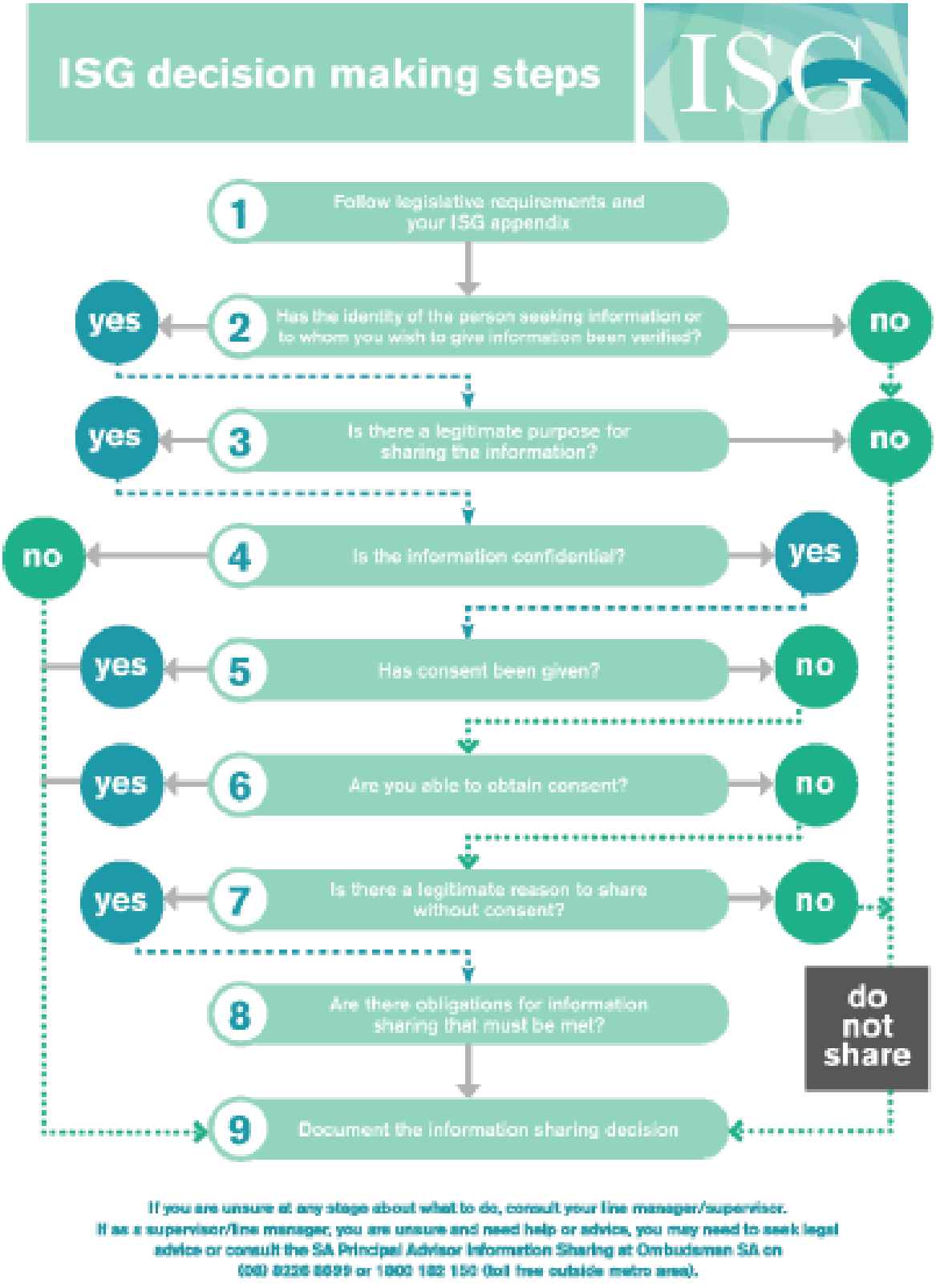
RELATED DOCUMENTS

- Code of Conduct Form
- Privacy and Confidentiality Agreement
- Policies and Procedures

REFERENCES

- National Standards for disability Services (2013)
- Disability Inclusion Act and Regulation 2014
- Privacy Act (1988)
- NDIS (Quality and Safeguards) Commission (2018)

APPENDIX : Information Sharing Guidelines



If you are unsure at any stage about what to do, consult your line manager/supervisor.
If as a supervisor/line manager, you are unsure and need help or advice, you may need to seek legal advice or consult the SA Principal Advisor Information Sharing at Ombudsman SA on (08) 8226 8699 or 1800 182 150 (toll free outside metro area).

ISG practice guide

1 Before proceeding, check your ISG appendix for guidance:

- share information in a manner that is consistent with legal obligations and organisational policies and procedures
- follow the ISG STAR principles to make information sharing Secure, Timely, Accurate and Relevant
- collaborate with other providers to coordinate services and manage/mitigate risk.

2 If you do not know the person seeking information or to whom you wish to provide information, you need to verify who they are and for whom they work before sharing information

3 You have a legitimate purpose for information sharing if you believe it is likely to:

- divert a person from offending or harming themselves
- protect a person or groups of people from potential harm, abuse or neglect
- protect service providers in situations of danger
- help service providers more effectively address risks to safety and wellbeing
- alert other service providers to an individual's need for assistance.

4 Generally, information is considered confidential when the person providing it believes it won't be shared with others

Assume that people will consider most information about themselves and their families to be confidential unless they have indicated otherwise.

5 Seeking informed consent is the first approach

This means the person understands the purpose for information sharing, with whom it will be shared, and what might happen as a result of sharing. If informed consent has been obtained, information can be shared.

6 It may be unreasonable to obtain consent if you are concerned that in doing so, the person might:

- move themselves or their family out of the organisation's or agency's view
- stop using a service seen to be necessary for the client or their children's safety or health
- coach or coerce a person to 'cover up' harmful behaviour to themselves or others
- abduct someone or abscond
- harm or threaten to harm others
- attempt suicide or self-harm
- destroy incriminating material relevant to a person or group's safety.

It may be impracticable to obtain consent if, for example, after reasonable attempts, you cannot locate the client. Discuss your concerns with a colleague/supervisor.

7 There is a legitimate reason to share information without consent if it is believed that failure to share information will lead to risk of serious harm

Disclosure of information without consent is permitted if:

(1) it is authorised or required by law, or

(2) (a) it is unreasonable or impracticable to seek consent; or consent has been refused; and

(b) the disclosure is reasonably necessary to prevent or lessen a serious threat to the life, health or safety of a person or group of people.

The decision to share without consent must be based on sound risk assessment and approved by the appropriate officer in your agency or organisation.

8 Situations where you must share information:

- eg you hold a suspicion, on reasonable grounds, that a child or young person has or is being abused or neglected, you must report this to CARL (131 478).
- eg you believe a person poses a serious risk to themselves or others, consider if you should notify SA Police (131 444) or *Mental Health Triage Services (131 465) (formerly known as ACIS).*

9 Keep records – particularly in relation to consent issues

As a minimum, document when sharing information is refused or occurs without consent. Follow your organisation's instructions about recording other significant steps.