

Safer Family Services

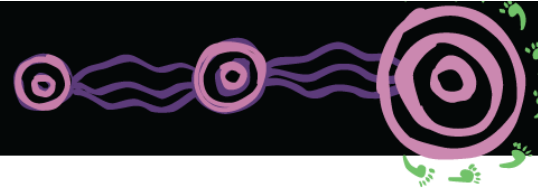
Practice Paper

Sharing information to promote the safety and wellbeing of children and families

Key messages

- Effective information sharing helps to ensure that vulnerable children and families receive support when needed and enables services to work in partnership to keep children safe.
- The *Children and Young People (Safety) Act 2017* (CYPS Act) and the *Information Sharing Guidelines for promoting safety and wellbeing* (ISG) provide a strong framework to support Safer Family Services' (SFS) practitioners to work collaboratively and share information with interagency partners to meet the safety and wellbeing needs of children and families.
- Where possible, practical and safe, the preferred approach to sharing information is with consent: however, the safety and welfare of a child or young person is a priority, and SFS practitioners are authorised to share information without consent in a range of circumstances. This includes when:
 - information is shared using the framework provided by the ISG to mitigate a risk of serious harm to a child or family member.
 - information sharing is required by law (such as reporting a reasonable suspicion that a child or young person is, or may be, at risk of harm under the CYPS Act, or in response to an application under the Freedom of Information Act 1991 or by order of a court or tribunal).
 - information is shared between specified persons and bodies under the CYPS Act to assist the recipient to perform a function or manage a risk relating to a child.
- SFS practitioners must be familiar with the pathways to share information and understand which pathway should be utilised in what circumstances. SFS practitioners should refer to the ISG processes and seek advice from seniors if there is any doubt about sharing information.





1. Discussing information sharing with families

Where it is safe, possible and practical, be open and honest with families that personal information may be shared with relevant agencies in order to best support the family and the safety and wellbeing of a child or young person. This is an important part of building trust, connection and a positive working relationship with a family.

Families should be made aware that their informed consent for the sharing of information will be sought and respected in all situations unless it is necessary to share the information:

- to prevent or lessen a risk of serious harm, abuse or neglect to a child or person,
- to prevent or lessen a risk of serious risk that a person may pose to themselves or others, or
- under legal requirements/obligations, i.e. mandatory reporting requirements.

The **IFS SFS consent to share information form** can be used to guide discussion with family about consent and to document when families consent to SFS sharing information with specific agencies.

Be open to hearing any concerns from families about their information being shared. Their views should always be considered carefully and balanced against the benefits of sharing their personal information.

Cultural considerations

When working with Aboriginal families, be responsive to the cultural factors that can influence communication and participation in the decision-making process. Cultural consultation is to be utilised from receipt of referral and at designated times throughout the intervention.

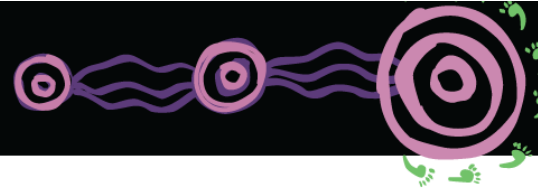
Be mindful of the community connections and the potential for harm if consulting across Aboriginal kinship systems and organisations broadly, without consent. The first step is to ask the family who to talk with to gain an understanding of their community networks.

Care must be taken to respond to any cultural and language barriers that impact effective communication and understanding of families from culturally and linguistically diverse backgrounds. If you are speaking with an Aboriginal person whose first language is not English, seek advice about appropriate communication protocols.¹ An interpreter may be needed to ensure there is clarity in all discussions and that families' wishes are heard and understood, and decisions and processes are made clear.²

¹ DHS, Assertive Engagement Practice Guide, 2021, pp. 6

² DHS, Interpreters and Translators Practice, 2021, pp. 3





2. Sharing information with consent

Where possible, practical and safe, the preferred approach to sharing information is with consent: however, the safety and welfare of a child or young person is a priority, and SFS practitioners are authorised to share information without consent in a range of circumstances to mitigate a risk of serious harm to a child or family member or when required under legislation.

Informed consent means:

- the person must be given enough information to make the decision (why is information sharing important, what may be shared and what will happen if consent is not provided)
- consent must be given voluntarily
- consent must be current and specific (seek consent again if the information sharing being considered is different to the original consent provided or if a significant amount of time has passed since consent was first given), and
- the person must have the capacity to understand and communicate their consent.

[Refer to the ISG](#) for more information about the key elements of consent.

Obtain consent from all family members

Wherever possible, consent should be obtained from all family members. Children and young people should be given the opportunity to be involved in the decision-making process in reference to information that is shared about them. Their level of engagement should be voluntary and based on their age, developmental level and any particular needs.³

Tailor the approach to seeking consent

Tailor your approach to meet the needs and capacity of the person you are seeking consent from. Issues that could affect an individual's capacity to consent include: age, physical or mental disability, temporary incapacity (i.e. during a psychotic episode or a temporary psychiatric illness), or limited understanding of English.

3. Sharing information without consent

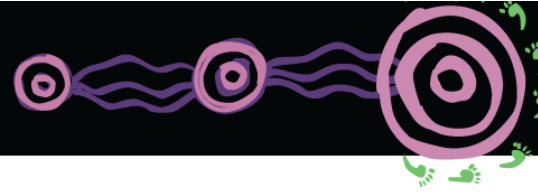
While it is preferred practice to obtain a person's informed consent to share information, this is not always a safe, possible or practical option. At times, the requirement to obtain consent may prevent or delay a service from engaging with a family or prevent services working collaboratively to best meet a family's needs.

SFS practitioners are authorised to share information without consent and including where consent may have been refused, in a range of circumstances. This may include when:

- information is shared using the framework provided by the ISG to mitigate a risk of serious harm to a child, family member or other person.
- information sharing is required by law (such as reporting a reasonable suspicion that a child or young person is, or may be, at risk of harm under the CYPS Act, or in response to an application under the Freedom of Information Act 1991 or by order of a court or tribunal).
- information is shared between specified persons and bodies under section 152 of the CYPS Act to assist the recipient to perform a function or manage a risk relating to a child (refer to 2.1 Sharing information under section 152 of the CYPS Act)

³ Ombudsman SA, Information sharing guidelines for promoting safety and wellbeing, Ombudsman SA, 2013, pp.10





Where safe and appropriate, SFS practitioners should inform a person at the earliest opportunity if their information has been shared without their consent (noting that any risk involved with informing them, should be assessed).

3.1 Sharing information under the ISG

The ISG provides a consistent, state-wide approach for information sharing when a person is believed to be at risk of harm (from others or as a result of their own actions) and adverse outcomes can be expected unless appropriate services are provided.

The ISG aims to:

- reduce the risk of service providers adopting conflicting information sharing practices
- increase the likelihood that the actions taken are based on a complete understanding of clients' circumstances and needs
- respect the privacy of individuals to the extent possible when furthering the aims above.⁴

Who can share information under the ISG

If there is a legitimate purpose for sharing information, the ISG supports information being shared with a broad range of other service providers including other government agencies, non-government organisations and Local Government Councils.

A decision to share information without consent or to refuse to share information must be approved by a supervisor or manager. The rationale for sharing without consent and the circumstances, are to be recorded in case notes in accordance with ISG guidelines.

When can information be shared without consent under the ISG

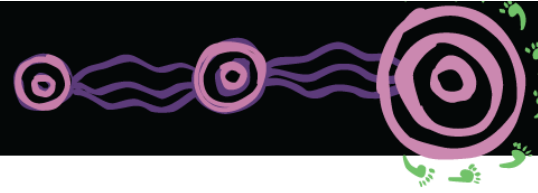
Under the ISG, it is possible to share information without consent, provided:

- it is unreasonable or impracticable to seek consent; or consent has been refused, and
- 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, and
- the procedures in the ISG are followed.

SFS practitioners must apply the nine decision-making steps to the ISG – see Appendix 1.

⁴ Ombudsman SA, Information sharing guidelines for promoting safety and wellbeing, Ombudsman SA, 2013, pp.1





4. Important considerations for information sharing

When making decisions to share information, either with consent, under the ISG, the CYPS Act or any other relevant legislation, the following important principles must be considered.

Follow the STARR principles

The 'STARR' principles provide a useful guide when making decisions to share information.

The STARR principles are:

Secure: information must be shared and stored securely

Timely: the sharing of information should not be delayed. Emergency requests should be clearly identified and actioned

Accurate: information shared should be accurate and clearly distinguish between facts and opinion

Relevant: the amount of information provided should be no more than the amount necessary to meet the purpose of the information sharing

Record: information sharing decisions must be recorded.

Verify the identity of the person information is to be shared with

Before sharing information, an SFS practitioner must verify the identity of the person they wish to provide the information to. To do this, a practitioner could:

- use government staff listings, global email lists, call the individual back at the organisation's number in the telephone directory and/or
- ring a senior person in the organisation to verify their role.⁵

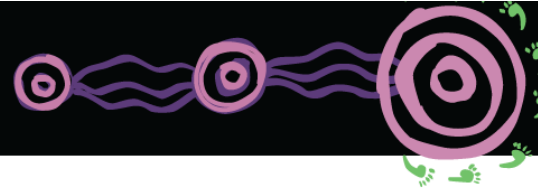
Exchange information securely

Information can be exchanged verbally (over the phone, in person or during a multi-agency discussion), or in writing (including email), provided it is done in a secure way. Some measures to ensure the confidentiality of information include:

- using email, store personal information in a password protected attachment and provide the password by telephone or subsequent email
- using registered mail where appropriate when posting letters and documents
- providing the recipient with information about the management of the information, including the limitations of how the recipient may use the information and confidentiality provisions applying to the information

⁵ Ombudsman SA, pp.7





5. Documentation and Record Keeping

SFS practitioners are required to maintain accurate records about information sharing and follow-up actions. Keeping accurate records is important for follow-up, referrals and interagency coordination, as well as accountability and risk management.

The following information should be recorded in response to each situation of information sharing

| | |
|--|--|
| <p>Information is shared with consent</p> | <ul style="list-style-type: none"> • Copies of written consent and/or file note of verbal consent recording: <ul style="list-style-type: none"> ○ who gave it, when and to whom ○ what the consent related to ○ information provided or received ○ outcome of any subsequent follow-up. |
| <p>Information is shared without consent</p> | <ul style="list-style-type: none"> • if consent was not sought, <ul style="list-style-type: none"> ○ why it was not possible or practical to obtain consent • if consent was sought, but refused, <ul style="list-style-type: none"> ○ the reason for this and why it is considered necessary to share the information without consent • what information was shared, when and by whom • the agency and the office or officer involved • outcome of any subsequent follow-up. |
| <p>Information sharing request is refused by SFS</p> | <ul style="list-style-type: none"> • the reason for SFS refusing to share information • if advice was sought from line managers or supervisors, what that advice was • outcome of any subsequent follow-up. |
| <p>Information sharing request made by SFS is refused by another service provider</p> | <ul style="list-style-type: none"> • the purpose of the request for information • the reason given by the external agency or service for the refusal • if advice was sought from line managers or supervisors, what that advice was • outcome of any subsequent follow-up. |

6. References

Child Protection Systems Royal Commission, *The life they deserve: Child Protection Systems Royal Commission Report, Volume 1: Summary and Report*, Government of South Australia, 2016

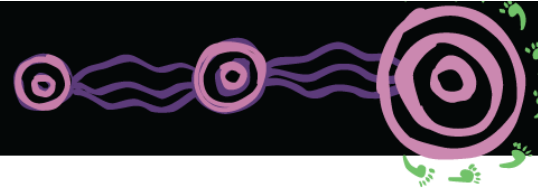
Department of Human Services, *Assertive Engagement Practice Guide*, 2021

Government of South Australia, *Children and Young People (Safety) Act 2017*

Government of South Australia, *Children and Young People Safety Regulations 2017*

Ombudsman SA, *Information sharing guidelines for promoting safety and wellbeing*, Ombudsman SA, 2013

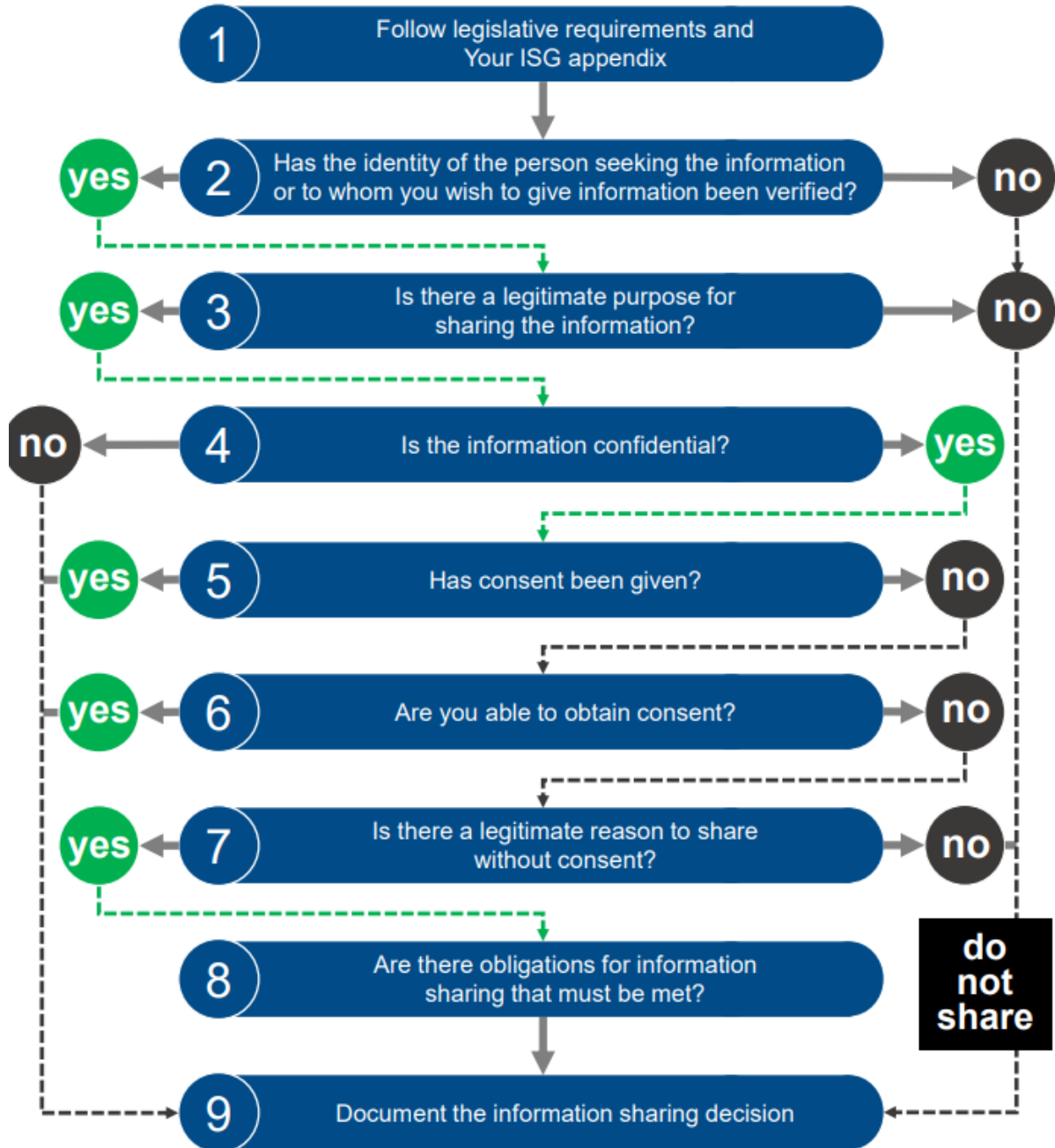


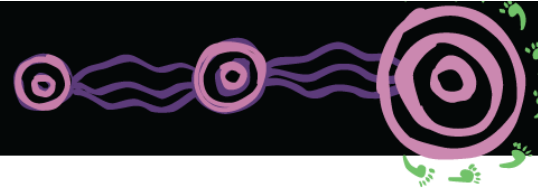


Appendix 1

ISG decision making steps

ISG





ISG practice guide

ISG

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 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 the 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 reasonable 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:

- e.g. 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 (13 14 78).
- e.g. you believe a person poses a serious risk to themselves or others, consider if you should notify SA Police (13 14 44) or Mental Health Triage Services (13 14 65).

9

Keep records – particularly in relation to consent issues

As a minimum, document when sharing information is refused or occurs with consent. Follow your organisation's instructions about recording other significant steps.

