Practice Guidance

Information sharing and confidentiality

Purpose

Information sharing is crucial to ensuring that children and young people are protected from harm and are supported to achieve their full potential. Sharing the right information in an effective and timely way assists the Department for Child Protection (DCP) and other services involved with children, young people and their families and carers to coordinate a better response and work collaboratively in a way that meets their needs.

The Child Protection Systems Royal Commission Report, *The Life They Deserve*, 2016 as well as other inquiries have consistently recognised the importance of collaboration and cooperation between agencies involved in service delivery to children. Caution about information sharing between government departments and non-government services has created barriers to meeting the needs of children and legislative change was recommended and implemented to address this.

The *Children and Young People (Safety) Act 2017* provides for information to be shared with a broad range of people and agencies, including government departments, local councils, statutory bodies, non-government organisations, and children and young people, their families and carers, where there is a legitimate reason to do so. This may include sharing information to assist an agency to provide services to a child or young person, or to manage risk to children and young people.

This guidance supports DCP staff to:

- share information and collaborate with others to promote the safety and wellbeing of children, young people, families and carers
- know when information must be shared, may be shared or should not be shared
- understand the interconnection between the *Children and Young People (Safety) Act 2017* and the Information Sharing Guidelines for Promoting Safety and Wellbeing (ISG) and how together, they provide a strong framework for appropriate information sharing
- understand the process and decision making steps that must be followed when sharing information; and
- ensure children and young people's right to safety is paramount in decisions to share information and is not overridden by other considerations such as privacy or confidentiality.

Scope

This practice guidance applies to all DCP staff and volunteers.

Key Steps / Contents

Guidance

1. Legal framework

The *Children and Young People (Safety) Act 2017* (CYPS Act) allows information to be shared with certain persons or bodies to perform functions related to providing services and support to children, when the information relates to health, safety or wellbeing of children and young people, or if it is necessary to manage risks to children and young people.

Sections 152 and 164 of the CYPS Act are the main legislative provisions for information sharing.

Additionally, the Chief Executive, DCP, has issued an authorisation permitting DCP staff to share information with any person where it is necessary to share the information to that person in order to protect a person from risk of serious harm; and the disclosure would not be inconsistent with the objects of the CYPS Act. Children and young people's safety must always be the paramount consideration.

These provisions are consistent with the Information sharing guidelines for promoting safety and wellbeing (ISG) which was developed as part of the South Australia Government's *Keeping Them Safe* child protection agenda. The ISG is implemented throughout government and relevant non-government organisations and it relates to information sharing for all vulnerable people, including children, young people and adults.

This guidance should be read in conjunction with the ISG.

1.1 Legislation that supports information sharing

Key sections of the legislation	
Section 152	Information may be shared with prescribed bodies (generally government agencies, local government organisations and NGOs who are funded by Government) to assist these bodies to perform official functions or to protect children and young people from harm.
Section 163	This section protects the details of people who have notified that a child or young person may be at risk of harm. Notifier details must not be disclosed unless one of the exceptions set out in s163 applies. An example of an exception includes the consent of the notifier.
Section 164(1)(a)	The sharing of information is allowed or legally required under the CYPS Act or any other law
Section 164(1)(b)	Sharing information with the consent of the person to whom the information relates. The approach to seeking consent from a child or young person should be tailored to their age and developmental capacity.
Section 164(1)(c)	This allows information to be shared with any person where that disclosure is connected to the administration or enforcement of the CYPS Act or any other Act. This has a broad application and will generally cover circumstances where the sharing of information will assist in making arrangements for the protection and care of children and young people.
Section 164(1)(d)	Information may be shared where the disclosure is made to: • a law enforcement agency (such as South Australia Police), or • a person or agency exercising official duties under an Act relating to the care or protection of children and young people

Section 164(1)(e)	Information may be shared with an agency or instrumentality of this State, the Commonwealth or another State or a Territory of the Commonwealth for the purposes of the proper performance of its functions.
Section 164(1)(f)	Sharing information where it is reasonably necessary for the protection of the lawful interests of the person disclosing the information. *This exception will only apply in rare circumstances and legal advice should be sought on a case by case basis before relying on this exception.*

2. Principles of information sharing

DCP encourages and expects that staff share relevant information promptly and appropriately as set out in the ISG and in line with the responsibilities and obligation of the CYPS Act. When sharing information, the following principles must be considered:

- Safety of children and young people is the paramount consideration
- People have a right to have their privacy protected
- Where privacy and risk to safety are in tension, responding to the risk always takes priority
- Sharing information must be in accordance with the CYPS Act and the ISG
- A person's consent to share information should be sought and obtained where safe, possible and practical. However, there are some exceptions to the requirement for consent.
- Information shared must be **Secure, Timely, Accurate and Relevant** (STAR principles):

  Secure: ensure records of information are shared and stored securely

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

  Accurate: ensure the information shared is accurate or advise of any variations that apply.

  Relevant: ensure the amount of information provided is no more than the amount necessary to meet the purpose of the information sharing.

It is good practice to discuss information sharing issues with senior colleagues. Where information is shared without consent, staff must obtain approval from a person with delegated authority (generally Supervisor or above).

3. Consent

Sharing information with consent underpins the development of engaging a positive working relationship with children, young people, their families and the services that support them and is the preferred approach for sharing information.

Unless the sharing of information is required by law, consideration **should always** be given to obtain consent if it is safe, appropriate and reasonable to do so.

3.1 Informed consent

Consent can be 'explicit' which means agreement is given verbally or in writing. Consent can be 'implied', which means information sharing is inherent in the nature of the service sought. Ideally, consent should be sought in writing using the DCP *consent to share* information form.

Gaining an individual's informed consent for information sharing should occur at the earliest possible point in an individual's engagement with DCP. Informed consent means:

- the individual is adequately informed before giving consent (e.g. understands why information sharing is important, whom it is designed to support and the desired outcomes)
- the individual gives consent voluntarily
- the consent is current and specific (revisit an individual's consent if the information sharing under consideration differs from the original examples discussed or if a significant amount of time has passed since consent was first given)
- the individual has the capacity to understand and communicate their consent.

The approach for seeking consent must be tailored for children and young people, individuals with cognitive impairments or individuals from culturally and linguistically diverse backgrounds

Consent can be evidenced by a written *consent to share information* form signed by the individual or a conversation that has been noted in a case note recorded to C3MS.

Always document consent on C3MS including details of who provided consent, what the consent related to, information sought/provided/received and any outcome or follow up.

3.2 Limited confidentiality – sharing information without consent

Individuals should also be informed at the earliest opportunity in circumstances where DCP may consider sharing a person's information without informing them or obtaining their consent. These circumstances include where:

- seeking consent may place someone at risk of harm
- it is impracticable or impossible to contact the person and the matter requires a prompt response
- a person is unable to consent because of age, developmental capacity or they have impaired decision making capacity
- where there is an intention to share the information even if the person has expressed, or is likely to express, a desire for the information to not be released (for example to assist a police investigation or a government agency to perform its official duties).

In some circumstances, it may not be safe, possible or practical to seek and obtain consent. Staff may use their use professional judgement to assess what is safe, practical and possible

and carefully consider the circumstances of the child and the family and the reason information is being sought. The reasons for not obtaining consent should be documented.

A decision to share information **without consent** or to **refuse** a request to share information requires the approval of a Supervisor or higher.

On C3MS, always document the rationale and decision to share without consent including why obtaining consent was unreasonable or impracticable, who approved the decision, what information was shared and when and with whom it was shared with.

4. Key considerations when sharing information

4.1 Cultural consideration

When working with Aboriginal children and young people and their families, staff must be sensitive and responsive to the cultural factors that can influence communication and participation in decision making process. Principal Aboriginal Consultants and Aboriginal Family Practitioners can provide advice and support, as required. For additional information refer to Working with Aboriginal and Torres Strait Islander Families Practice Guide and South Australian Aboriginal languages interpreters and translators guide.

Consideration must also be given to the relevant cultural perspectives and beliefs when working with children and young people and their families from culturally and linguistically diverse (CALD) backgrounds. If English is not, the person's first language, additional time or a more flexible approach may be needed to support their participation and ensure they have access to an interpreter if required.

Additionally, the ISG provides valuable information and about guidance sharing information in a culturally sensitive manner (see page 21 of the ISG for *additional considerations when working with Aboriginal or culturally and linguistically diverse families and communities*).

4.2 Consider if the information is 'personal' or 'confidential'

First consider whether the information intended to be shared is personal and/or confidential.

Personal information means information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion[1].

It is best to assume that people will view most information about themselves and their families as confidential unless otherwise indicated during discussions.

4.3 Consider if there is a legitimate purpose for sharing the information

Staff must always be satisfied that they have a legitimate purpose to share or receive the information. A legitimate purpose exists if there is a real and valid reason for sharing the information, there is an authority to share the information (e.g. under the ISG and CYPS Act), and it is reasonable to do so in the circumstances.

To help make a decision, the following questions should be considered:

[1] *Government of South Australia, Information Privacy Principles*

- In what way is this information intended to help prevent harm?
- What specific information is relevant (needed) to achieve that?
- Whose identities must be disclosed as part of the specific information, and whose identities can be kept confidential?
- Is there a legal obligation to share the information?

If unsure about whether a legitimate purpose for sharing information has been established, staff should seek advice from their Supervisor, Manager or DCP Legal Services Unit.

4.4 Verify the identity of the intended recipient of the information

Staff should never provide information to another person or agency unless they believe there is a justified reason and they have verified the identity of the person requesting information or the person to whom information will be provided.

Requests for information sharing may have a level of urgency and be made via the phone. Unless staff have an existing working relationship with the person making the information request, care must be taken to establish the identity of the person and their role in their organisation and staff must verify the requester's identity. To verify the identity of a caller, ask the person to hang up, look up the organisation's phone number, ring this number and ask to speak to that person.

If you believe someone has deliberately misrepresented themselves in seeking information, the SA Police must be contacted as it may represent an offence.

4.5 Consider any restrictions on sharing the information

When assessing whether to share information, staff should consider whether there is any reason why the information should not be shared. For example, the information may be protected by legal professional privilege or prohibitions in the CYPS Act or other legislation, its release may endanger a person's life or it may unnecessarily identify a third party (such as a voluntary reporter or service provider).

Staff must be mindful that Section 163 of the CYPS Act prohibits the disclosure of the identity of a person who has made a report or notification to any other person unless the disclosure is:

- made with the consent of the person who gave the notification; or
- required or authorised by the Chief Executive or under the CYPS Act; or
- made by way of evidence in proceedings before a court or tribunal and where the court or tribunal has permitted that disclosure; or
- authorised by the Children and Young People (Safety) Regulations 2017.

Even if information is required by law, care should be taken to ensure that the provision of such information does not contravene any other provision under the Act. For example, a subpoena may compel the production of information relating to a child but anything that may identify a notifier of suspected or actual child abuse or neglect must not be shared.

5. When information MUST be shared

In some circumstances, it is mandatory that DCP share information with another person, organisation or body. This includes where it is required by the CYPS Act, another law (such as the *Freedom of Information Act 1991*) or by order of a court or tribunal.

Where there is a mandatory requirement to share information, staff are not required to seek the consent of the person to whom the information relates. However, staff must still apply best practice and the information sharing principles outlined in this Practice Guidance.

Circumstances in which information **must be shared** under the CYPS Act are:

- A mandatory notifier must report a suspicion that a child or young person is at risk of harm to DCP
- A child or young person who is to be placed with an approved carer is first entitled to be provided with information in relation to the approved carer
- Approved carers are entitled to any information about a child or young person and their circumstances that may be relevant to their carer's decision of whether to accept the placement
- Approved carers are entitled to any information (including medical reports) held by the agency that is reasonably necessary to ensure that they are able to provide appropriate care to the child or young person in all of their circumstances; and the safety of the approved carer and any other member of the approved carer's household.

If a staff member is unsure whether they have a legal obligation to share information under to the CYPS Act, another Act or order of a court or tribunal, they should seek advice from their Supervisor, Manager or DCP Legal Services Unit.

6. When information MAY be shared

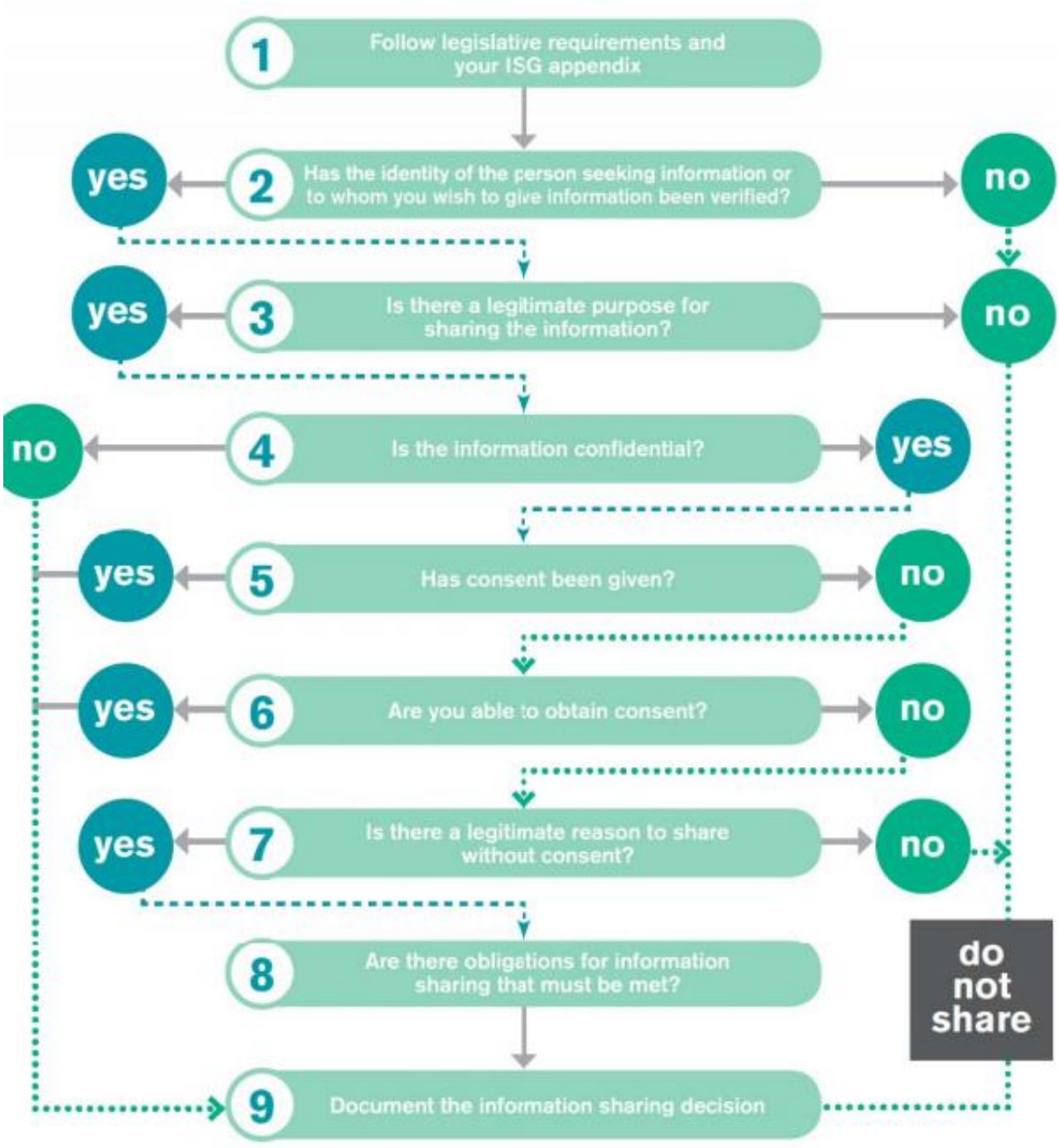
Information may be shared in many circumstances including managing risk, facilitating the coordination of services to meet the care and protection needs of a child or young person, or to assist agencies to perform functions including providing services to children and young people and their families that meet their needs, and are culturally appropriate and safe.

The Chief Executive, DCP has authorised staff to share information to any person where:

- it is necessary to disclose the information to that person in order to protect a person from risk of serious harm; and
- the disclosure would not be inconsistent with the objects of the CYPS Act (children and young people's safety must always be the paramount consideration).

Where these conditions are met, staff **must** follow the nine ISG decision making steps and this practice guide when sharing information outlined below.

ISG decision making steps



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 128 150 (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.

6.1 ISG decision making steps and practice guide

ISG Step 1: Follow legislative requirements and the ISG

The CYPS Act and the ISG provide a strong framework for sharing information. Staff must comprehensively understand the information sharing provisions under the ISG, as well as the CYPS Act as outlined in this practice guide.

ISG Step 2: Has the identity of the person seeking information or to whom you wish to give information been verified?

Staff must always verify the identity of the proposed information recipient to ensure information is appropriately and securely shared and not misused. If you do not know the person seeking information then you must verify who they are and for whom they work for before sharing information.

Refer to the information section "4.4 Verify the identity of the intended recipient of the information" in this practice guidance and page 13 of the ISG for more information.

ISG Step 3: Is there a legitimate purpose for the sharing of information?

Staff must be satisfied that there is a legitimate purpose for sharing the information. You have a legitimate purpose for sharing information under the CYPS Act and the ISG if the information is likely to manage risk or help service providers to manage risks to safety and wellbeing, protect service providers in situations of danger, or divert a person from offending or harming themselves.

Refer to the information "*4.3 Consider if there is a legitimate purpose for sharing the information*" as well as in this practice guidance and page 13 of the ISG for more information.

ISG Step 4: Is the information confidential?

Generally the term confidential applies to information that is provided by an individual who believes it will not be shared with others. This assumption of confidentiality underpins all interactions with DCP service users.

The aim of sharing information under the ISG is to help protect children, young people, their families and members of the community from current or anticipated serious threats to their wellbeing or safety and to do so with the client's consent, wherever it is safe and possible to do so. Individuals must be informed of confidentiality limitations. This means it is explained to them when and why it may be necessary to share their information with or without their consent.

The following statement can be used in discussion when advising individuals of the limits of confidentiality, their right to privacy and explaining the duty of care incumbent on DCP practitioners:

- We will seek your consent to share your information wherever it is safe and possible to do so. In certain circumstances your information may be provided to other agencies or organisations without your consent in order to protect you and others from serious threats to health or safety or if we are required or authorised by law to do so.

See page 14 of the ISG and the information and "*4.2 Consider if the information is 'personal' or 'confidential"* in this practice guidance for more information.

ISG Step 5: Has consent been given?

Seeking informed consent should be considered in the first instance unless it is not safe, is not appropriate or is not reasonably practicable. Informed consent 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.

Refer to the information under "*3 Consent*" in this document for more information.

ISG Step 6: Are you able to obtain consent?

Consent must be sought wherever it is safe, appropriate and practicable to do so.

Refer to the information under "*3.1 Informed consent"* in this document for more information.

ISG Step 7: Is there a legitimate reason to share without consent?

It may be unreasonable to obtain consent in some circumstances where there are concerns which may include a person attempting to harm themselves or others, abducting someone or absconding, or coaching or coercing a person to cover up harmful behaviour. Refer to page 17 of the ISG for further information.

When assessing if there is a legitimate reason under the ISG to share without consent, staff must confirm the purpose for which they are sharing the information without consent is to promote the safety and wellbeing of children, young people and their families. In making this assessment staff should refer to the information under "*3.2 Limited confidentiality – sharing information without consent"* in this practice guidance.

If information is to be shared for a purpose other than to promote the safety and wellbeing of children, young people and their families, information cannot be shared under the ISG and this pathway. Consider whether information can be shared under "*5 When information MUST be shared"* of this practice guidance.

ISG Step 8: Are there any obligations for information sharing that must be met?

There are circumstances where information must be shared under the ISG. These include if there is a reasonable suspicion that:

- a child or young person has or is being abused or neglected - you must report this to CARL (131 478)
- a person poses a serious risk to themselves or others - consider if SA Police (131 444) or Mental Health Triage Services (131 465) should be notified.

In addition to mandated notifier requirements, the CYPS Act requires information to be shared with children and carers when placing a child or young person. For further information refer to "*5 When information MUST be shared*" of this practice guidance.

Staff must consider whether any of these circumstances exist before sharing information to determine if information is being shared under the ISG or the CYPS Act.

ISG Step 9: Document the information sharing decision

Decisions to share (or not to share) information must be appropriately recorded, including the approvals obtained and any follow up actions. See also page 18 of the ISG for further information.

Information sharing situation	What to record	Where and how
Information is shared **with consent**	Copies of written consent and/or file note of verbal consent recording: • who gave it, when and to whom • what the consent related to • information sought, provided or received • outcomes and follow-ups	Any information shared with consent must be recorded in C3MS, including a copy of the signed *consent to share information* form if consent was provided in writing.
Information is shared **without consent**	• Risk assessment • Why obtaining consent was	Any information shared without consent must be recorded in

	unreasonable or impracticable • Line Manager's approval, if required • What is shared, when and by whom • the agency and the office or officer involved (receiving and providing) • outcomes and follow-up	C3MS.
Information sharing request is **refused**	• the purpose (the immediate or anticipated risk the request was intended to address) • reason given for refusal (risk assessment) • approval from line Manager • outcome of any subsequent follow-up	Decisions not to share information must be recorded in C3MS.

6.2 Additional legislation consideration

Additionally, Section 164 of the CYPS Act provides that information may be shared where it is:

1. authorised by or under this Act or any other Act or law
2. with the person's consent
3. in connection with the administration or enforcement of the CYPS Act or any other Act
4. for the purposes of referring the matter to a law enforcement agency, or a person or agency exercising official duties under an Act relating to the care or protection of children and young people
5. to an agency or instrumentality of this State, the Commonwealth or another State or a Territory of the Commonwealth for the purposes of the proper performance of its functions
6. reasonably necessary for the protection of the lawful interests of that person.

Where applicable, staff must also adhere to specific practice guidance. For example:

- Gathering information to assess and manage risk practice guide (s150 and 152)
- Interstate transfers of child protection orders and proceedings practice guide (s142)
- Provision of information to care leavers practice guide (s153)
- Chief Executive requiring State authority to provide a report practice guide (s151)

7. When information SHOULD NOT be shared

In some circumstances, certain information must or should not be shared. This includes (but is not limited to) where:

- the information discloses the identity of a notifier
- there are provisions in other legislation which prohibit the disclosure of part or all of the information (such as section 67E of the Evidence Act 1929)
- the information is protected by legal professional privilege or

- the information is protected by public interest immunity.

If staff are unsure whether there is a legal or other good reason why information should not be shared, consultation with their Supervisor, Manager or DCP Legal Services Unit should occur.

Decisions not to share information must be recorded in C3MS, including the purpose and detail of information requested, reason given for refusal to share, the approvals obtained not share and any follow up actions.

8. Managing disagreements about information sharing

Disagreements about information sharing can occur:

- Between DCP staff
- Between DCP and another agency or professional

Where a disagreement occurs, staff should seek advice from their line Manager or another senior member of staff. Where the matter is still not resolved, they may choose to raise this with the Regional Director or seek advice from DCP Legal Services Unit.

If a service provider refuses to share information, staff should ask or provide further information about their concerns and why the information sharing is necessary. It is reasonable for staff to ask to speak to the person's Supervisor, and/or seek support from their Supervisor or another senior colleague.

9. Secure management of personal and confidential information

Where information is shared with other people, it is important this is done sensitively and respectfully. Only information that is relevant to the purpose for which the information is being shared should be provided, remembering the paramount consideration is ensuring children and young people's safety.

It is sometimes necessary to provide written information to other people; for instance where making a referral. Every effort should be made to ensure only the relevant person or organisation is given access to the information. Some simple measures to ensure the confidentiality of information are:

- delivering reports and referral forms personally and directly to the intended recipient
- using registered mail where appropriate when posting letters and documents
- when using email, confining personal information to an attachment that is password protected and providing the password to the recipient by phone
- including information for the intended recipient regarding expectations about the management of personal and confidential information.

Roles and Responsibilities

Role	Authority/responsibility for
All DCP staff	Adhering to this practice guidance and the ISG
Supervisors	Adhering to this practice guidance and the ISG Approving decisions to share information without consent
Managers	Adhering to this practice guidance and the ISG Approving decisions to share information without consent
DCP Legal	Adhering to this practice guidance and the ISG Providing legal advice as required

Glossary

Term	Meaning
Confidential	Information provided in confidence and which is assumed, by the individual who provided it, that it will not be shared with others.
Information	Written, verbal or electronic reports and accounts, including fact and opinion.
Informed consent	Permission an individual gives to information sharing, either implied or explicit, after they have demonstrated they understand the purpose of the request and the likely outcomes of that consent. Age, intellectual capacity, mental health and abuse of substances will each impact on an individual's capacity to demonstrate this understanding and these impacts must be acknowledged – they cannot be 'overlooked'.
Personal information	Information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion
Practicable	Capable of being done or put into practice; feasible.

Authority

Children and Young People (Safety) Act 2017
Children and Young People (Safety) Regulations 2017
Information Sharing Guidelines for Promoting Safety and Wellbeing (ISG)

Document control

Publication date	1 November 2019
Replaces	*Disclosing personal information guideline (22 October)*
Accountable Director (name and position)	Mel Bradley, Director, Quality and Practice
Accountable Director (phone)	8226 2840
Lead Writer (name)	Rebecca Carrigan
Applies to	All staff
Approved by	Policy Governance Committee
Approval date	1 November 2019
Commencement date	11 November 2019
Review Date	11 November 2021
Risk Rating	High

REVISION RECORD		
Date	**Version**	**Revision description**

Appendices

1. Consent to share information form
2. Information Sharing Guidelines for promoting safety and wellbeing (ISG)