

Accident and Incident, Investigation, Reporting and Critical Incident Procedure

Scope

To implement an incident investigation program that focuses on recordable injuries, illnesses and near miss and minor incidents.

Purpose

The purpose of incident investigations is to determine the “root cause(s)” of an incident, so that corrective action can be taken to eliminate or control specific hazards. Through the investigation of incidents, the Tailem Bend Community Centre Inc. (TBCC) is able to analyse and learn about causes, which in turn will give better control of incidents.

General

This process is a guiding tool to use when implementing the incident investigation program

1 Incident definition:

All incidents should be reported. Those with serious potential should be selected for further investigation. A serious or serious potential incident is one that either results or could reasonably result in:

- 1.1 An injury or illness involving lost or restricted activity to any person, including volunteers, students and employees.
- 1.2 A significant spill or release of chemical or product
- 1.3 Significant damage to buildings or equipment
- 1.4 Critical Incidents – significant negative impact to health, safety or wellbeing of a client.

2 First Aid Incidents

First aid cases must also be investigated and reported: although not in as rigorously a manner as major incidents.

3. Critical Incident definition

The Chief Executive Officer (CEO) is responsible for determining if a specific incident is to be classified as a Critical Client Incident.

Critical Incident is an event (or alleged event) that occurs as a result of, or during the delivery of services directly provided or funded by TBCC, and has caused or is likely to cause negative impact to the health, safety or wellbeing of a client or service recipient.

Critical client incidents may include but not limited to;

- 3.1 Un-expected death, serious injury or alleged assault (including physical, sexual abuse, of services
- 3.2 Serious unlawful or criminal activity or conduct that has potential to cause serious harm to another
- 3.3 As serious fire, natural disaster, accident or other incident which will, or is likely to prevent, service provision, or which results in closure or significant damage to premises or property, or which poses a significant threat to the health and safety of clients.

The assessment of whether an incident should be treated as a critical client incident should take into account the following:

- The extent of harm that resulted, or may result
- The likelihood that others may be affected
- The death, serious injury or harm has an obvious and direct correlation to the services the person was receiving
- The death, serious injury or harm is due to unusual circumstances
- The duty of care that may be expected of the department and /or the funded service provider in relation to the incident

DISCLOSURE: *providing information about a critical incident to others not directly involved in the incident, but who may be affected, either directly or indirectly (for example, family member's of the affected client, other clients who may have been harmed and / or their families). Please note that meeting reporting requirements (for example, mandatory notification, reporting to SAPOL) does not constitute disclosure. Disclosure decisions must take into account the potential for others to have been affected or harmed, the potential for others still to be at risk of harm or require assistance to alleviate the effects of harm; and risks in disclosing information. They must also take into account what information will be provided, to whom, for what purpose and with what justification, in what format and appropriate approval mechanisms.*

4. The Incident Investigation Process

The incident investigation process contains 5 steps:

1. Gather Information
2. Determine Causes (direct and indirect)
3. Corrective Action(s)
4. Communication
5. Document
6. Report
7. Follow-Up

Step 1- Gather Information

Before beginning this process, it is very important to have the correct people involved to perform an investigation, they should include but not be limited to:

- 4.1.1 CEO
- 4.1.2 Injured or involved person(s)
- 4.1.3 Witness

The initial investigation should take place at the scene. The investigating team will be able to examine the scene and visually see what took place. It is critical to document what was said and observed.

Tailem Bend Community Centre Inc. will use the following reporting forms:

- Consent relevant to activity – including volunteer registration form, program or service registration and consent form.
- Information Sharing Form

Step 2- Determining Causes (Direct and Indirect)

As the investigation team gathers information from an incident, it is important to investigate the behaviours involved in an incident. Remember, between 90 and 96% of all injuries that occur in industry are related to a person's own behaviour.

Behaviours fall into two categories direct or indirect. Direct causes are usually easily identified, and in most cases the incident investigation stops here. However, indirect causes require more effort to bring to the surface and this is usually an indication of a breakdown in a management system (i.e. procedures not being up-to-date, taking shortcuts to get a job task completed, etc.).

To better illustrate direct and indirect here is an example: A volunteer was running to the lunch room and slipped on a water spot that was on the floor and injured themselves. Most investigations would identify the volunteer running and the water as the direct cause to the incident and in most cases, the investigation would stop here. However, you have not identified the “root cause” of the incident. You need to find out where the water came from, and let’s say it was a leak from the refrigerator. The indirect causes would be the refrigerator. Unless you correct the leak, you will not eliminate the incident from occurring again within your facility. So, to identify direct and indirect causes, it will require the investigating team to ask detailed questions and not be satisfied with first general impressions.

Step 3- Corrective Actions

Once the investigation team completes the investigation and generates a report that identifies how the incident occurred, direct and indirect causes, the next step is to identify corrective actions that will address the incident. Corrective actions that require little time to execute should be done immediately. However, situations where the corrective action is more involved (i.e. ordering materials etc.), the recommendations should involve a short and long range plan. These recommendations should be tracked to ensure closure.

Communication

Once the incident investigation report has been completed and corrective actions identified. It is important to communicate the incident report with the Management Committee when a serious injury (i.e. WH&S incident, near misses that had the potential for serious injury and/or property damage that exceeds more than \$500.00). The purpose of communicating and sharing incident investigations is that the potential for the same incident to occur is lessened. Also, the name of the injured volunteer/student/visitor etc. should be removed when communicating incident reports.

Follow-Up

The final step (follow-up) is where a lot of incident investigation programs fail. Once an investigation has been completed and corrective actions identified most investigations stop here. The reason for this is that we fail to monitor corrective actions and they fall through the cracks. It is vital to the incident investigation process to develop a tracking system that will give you the capability to see what corrective items have not been completed. By having a monitoring system that tracks closure will ensure a successful investigation program.

Reporting Requirements

Anytime the Tailern Bend Community Centre Inc. encounters a serious WH&S Recordable or Environment Incident, the centre must place a copy of the investigation report on file. Every incident must be entered into the TBCC Risk Hazard Incident register and be reported to the Board by the next full Committee Meeting.

Critical Incident Reporting

Critical Incidents must be managed in accordance with Department of Human Services Critical Incident Policy and the Department of Health Serious Incident Response Scheme (SIRS) Policy and Incident Management System.

SAPOL reporting

Non-government organisations need to be aware of their responsibility to report serious incidents to South Australia Police (SAPOL). An incident must be reported immediately if:

- it is a serious concern or a criminal offence (for example, rape, unlawful sexual intercourse, indecent assault, aggravated physical assault, significant client abuse)
- there is a need to preserve physical evidence (for example, medical or scene examination, seizure of clothing)
- there is a serious risk to the safety/security of any person(s) on site or
- a person has an obvious injury resulting from an offence, or complains of an injury that may not be obvious but is considered reasonably likely to have occurred.

Other incidents of concern that, after consideration, are felt to require police intervention should be reported as soon as reasonably practicable.

Serious care concerns should be reported directly to:

Care Concerns Investigation Unit
Telephone +61 8226 8441
Email DCPCareConcernManagementUnit@sa.gov.au

Call DCP After Hours on 13 16 11 for after hours child protection and urgent matters requiring DCP support.

DHS reporting

DHS implemented a critical client incident policy in 2014 to improve the handling of critical client incidents. The policy has recently been updated. The policy aims to support the safety and wellbeing of clients and ensure that critical incidents affecting DHS clients are effectively responded to, managed and reported. Please report critical incidents to:

Team Leader Disability, SA Feedback and Incident Review team
Telephone +61 8 8207 0490
Email DHSIncidentManagementFeedbackandIncidentReview@sa.gov.au
Reporting incidents to SA Police by non-government organisations

Reporting Process

The following outlines the process that must be followed in relation to all Critical Client Incidents.

The initial notification if (Co not available by telephone) may be via email and must include the words Critical Client Incident in the header, and provide the following information:

- Date and Time of the Critical Incident
- Location of the Critical Incident
- Details about TBCC or the Member Organisation: address and contact details.
- A succinct summary of what happened including, the relationship of any alleged perpetrator (s) to the alleged victim (s)
- The immediate steps that were taken to address the situation
- Current safety issues (i.e. is the client safe?)
- Coordination requirements (e.g. with other agencies, other areas of the department)
- Staff must ensure that they comply with any other external mandatory reporting requirements and record when it occurs.
- In the case of a reportable death that is deemed a Critical Client Incident, staff MUST also refer to Coronial Policy.

- DHS Critical Client Incident Manager may be required to advise other key stakeholders, on an as needs basis, after further assessment of the incident.

Reporting: Those involved in or aware of the incident must adhere to any mandatory or legislative reporting requirements within the appropriate timeframes, and any other statutory guidelines and procedures for incident management.

These reporting requirements may include, but are not limited to:

- Reporting an alleged offence to SAPOL
- Reporting suspected abuse or neglect of a child to the Child Abuse Report Line (CARL)
- Reporting all coronial matters consistent with legislation and Departmental Coronial Policy
- Reporting to the Health and Community Services Complaints Commissioner
- Reporting notifiable work-related injuries, fatalities or a dangerous occurrence to Safe Work SA

In the case of a death, the Critical Client Incident Manager MUST refer to the DHS Coronial Policy and Guidelines.

A disclosure must be undertaken for all Critical Client Incidents.

This assessment takes into account the potential for, a likelihood that, others (for example, other current or former clients) have been affected and / or experienced harm, or the potential for others to be still at risk of harm or require assistance to alleviate the effects of harm.

Disclosure decisions must also take into account the risks in disclosing, or not disclosing, information; and the potential impacts of disclosure. If the assessment indicates disclosure may be warranted, consideration must also be given to any constraints or limitations on disclosure (for example, the timing of an investigation by SAPOL or another body); appropriate parties to receive a disclosure; and managing the disclosure process.

Incident closure/ downgrading: At the discretion of TBCC CO and Incident Manager, an incident may be downgraded or closed as a critical client incident (for example, when the initial crisis is passed and the situation has stabilised sufficiently to be managed with existing processes and procedures).

- The Critical Client Incident Manager will provide information to TBCC CO and recommend that a matter be downgraded or closed
- The Critical Client Incident Manager, in consultation with TBCC CO will make a decision and advise Renewal SA and relevant authorities where appropriate.

Review: TBCC will review the information gathered as a result of the critical client Incident with the aim of improving service quality and minimising risks.

Follow – up Action

Record details of Critical Client Incident

- The CO staff and Volunteers involved in the incident must record all details related to the incident as it occurred, as soon as practical. The following information should be included in any notes made by staff. The information is the same as initial reporting.

Counselling and Debrief Sessions

Staff and clients involved in the incident should be encouraged to seek counselling and support as appropriate. Confirm this suggestion in writing. Where appropriate a staff debriefing should take place.

Role of the Critical Client Incident Manager

1. A Critical Client Incident Manager must be appointed by TBCC to supervise and manage the incident to its conclusion and to provide a single point of contact and coordination, including for DHS
2. The Critical Client Incident Manager is responsible for:

- Overseeing the management of the incident, including cross- departmental and cross-agency coordination, and monitoring SAPOL investigation and court proceedings where required.
- Ensuring a report outlining the details of the incident and relevant background is provided to DHS as soon as possible or as negotiated, of TBCC becoming aware of the Critical Client Incident.
- Ensuring that clients and staff involved in the incident have been encouraged to seek counselling and support
- Providing regular updates to the Board of Management and DHS
- Recommending to the Board of Management when the matter can be downgraded or closed.

Governance or Board Reports

- The CO is responsible for the coordination and preparation of any Governance or Board Reports
- As required, the CO will report to the TBCC Chairperson and any reportable incident will be recorded at the next Board Meeting

Review

Analysis of the Critical Client Incident

- After the closure of the Critical Client Incident TBCC will undertake an internal review. The CO will appoint a Reviewing Officer.
- A government body (SAPOL or Safe Work SA) may also undertake an external review
- The purpose of the internal review is to avoid any similar events in the future by identifying characteristics that may have led to the incident
- The Reviewing Officer will hold discussions and interviews with witnesses or others that may have been involved in the incident, as well as identifying any physical attributes that may have assisted or caused the CCI; such as a car, trailer, electricity, tools or water.
- List the ways in which your organisation will prevent similar incidents
- The Reviewing Officer will provide the CO a Summary Report and any recommendations. This report will also be provided to the TBCC Board.
- If requested, the report may be provided to DHS

Record keeping

Existing service recipient / staff files will be used to record details of information sharing decisions and actions.

Records of information sharing are essential:

- When information is shared with consent - evidence should be recorded on a consent form, registration form or similar, or recorded as a file note.
- When information is shared without consent, or
- When information sharing requests are refused by the organisation, or to the organisation, it should be recorded on the Information Sharing Record.

Information sharing situation	What to record	Where to record
1. Information is shared with consent	Copies of written consents and file note of: <ul style="list-style-type: none"> •verbal consent recording •who gave it, when and to whom •what the consent related to •information sought, provided or received 	<ul style="list-style-type: none"> •Record on consent form relevant to area of activity or as a file note. Filed in securely maintained records management system – Service Recipient /Staff file.
2. Information is shared without consent (by the organisation or to the organisation).	<ul style="list-style-type: none"> •staff/volunteer involved •referred to TBCC CEO •advice received from others (including staff at the Child Abuse Hotline) •why consent was not obtained •what information is shared, when and by whom •outcomes and follow up 	<ul style="list-style-type: none"> •Record information on Information Sharing Record and store in Service Recipient /staff file
3. Information sharing	<ul style="list-style-type: none"> •staff/volunteer involved 	

request is refused (by the organisation or to the organisation).	<ul style="list-style-type: none"> •referred to CEO •the purpose (the immediate or anticipated risk the request was intended to address) •reason given for refusal •outcome of any follow up 	
---	--	--

6. Cultural Guidance

TBCC Inc. recognises the diversity of people within the community. The organisation also recognises that where people have different cultural beliefs, the approach to service or program delivery may need to be different. For example, in many Aboriginal groups, sisters may be the daughters of an aunt and an aunt may be the person responsible for guidance and discipline, meaning in some cultures those with the authority to give consent may not be who you would expect. There may also be significant repercussions within a community and for other workers from the same cultural background as a result of seeking consent or sharing information.

Cultural factors however, do not excuse behaviour that affects disadvantaged people or places them at risk of harm, abuse or neglect. It is important to guard against cultural stereotypes both positive and negative. Staff should seek advice if they are involved in information sharing actions involving families whose culture is unfamiliar to them. In South Australia there are a range of organisations and resources that may assist staff to make decisions and provide services that are culturally appropriate.

7 Case studies

The following case studies provide examples in the context of the organisations programs and services of how to apply the ISG including:

- when not to share
- when to share
- when to request information
- what processes to use (for example documentation)
- how to go about seeking consent
- key contact people and resources – only the TBCC CEO can approve information sharing without consent).

The diversity of programs and services of the organisation means that these are only a small sample, always seek advice if unsure, how these guidelines could be applied to a specific situation.

Case study 1

Sharing is justified - information sharing without consent ensures a service recipient receives appropriate support

Mary is a 78 year old woman who uses the Council bus driven by a volunteer to do her weekly shopping. Mary's husband has advanced Alzheimer's disease and lives with Mary in their home they have shared for 50 years. When the driver goes to pick Mary up one day he observes that her husband is tied to the chair in the house. Mary says if she doesn't do this she cannot go shopping, as she worries that her husband will wander off while she is away. Volunteers also observe Mary has been losing weight and often talks about 'ending it all.' Volunteers suggest that the organisation may be able to provide some assistance in the form of company for her husband while she shops and that there may be assistance through the Council or Community Health that would further support her. She says, "don't be silly I can manage", but appears to be very withdrawn, the volunteer pushes the issue and Mary becomes upset and does not want to talk about the subject any more, she says "don't say anything - 'they ' will put us in a nursing home, I would rather die!" The volunteer reports this information to the CEO who decides it is important to go against Mary's wishes and contacts the Council and local Community Health Service.

The Health Service staff visit Mary and reassure her that they are there to help, a Dementia Care package is set up, which provides support for Mary and her husband in practical and emotional ways. The organisation continues to provide transport.

In this case, there is sufficient reason to share information without Mary's consent, to reduce the risk of harm to her husband and to herself and for them to receive appropriate support. The CEO recorded the decision to share information without Mary's consent on the Information Sharing Record and filed it in Mary's file, including the outcome.

Case Study 2

Sharing is not justified – information sharing without consent is not justified due to a lack of risk to safety or well-being.

A 16 year old girl, participates in a TBCC exercise program. She is seeking to lose weight and become fitter. She has not disclosed any difficulties or concerns about her relationships with her peers or with adults. The trainer identifies that she is a little over the normal Body Mass Index (BMI) and seems committed to a healthy fitness and eating regime.

The counsellor at the school where the girl attends is aware of the girl's involvement in TBCC's program but not the specific program or reasons for accessing the service. She has refused to provide this information. The counsellor believes he can provide better support to the student if he knows what issues the girl is facing and seeks this information from the CEO. The girl is coping well at school, both academically and socially.

The CEO liaises with the trainer and decides that if information is not shared by him it is reasonable to believe that neither the girl nor others will be 'at increased risk of harm'. The basis for declining to share information is explained to the counsellor and a record of this refusal is kept in the program service recipient files.

There was no justification for sharing information without consent as the safety or well-being of the girl was not at threat.

5 Information Sharing

The *Information Sharing Guidelines for Promoting the Safety and Well-being of Children, Young People and Their Families* (ISG) are the overarching information sharing principles and practice for all relevant government agencies and non-government organisations (NGOs) in South Australia. Mid Murray Support Service Inc. 59A. ISG Appendix is linked to and should be read in conjunction with the ISG and provides direction for the implementation of the ISG.

Refer to the following documents

- ISG Practice Guide and decision making steps
- TBCC Information Sharing Guidelines and consent form V1

These two documents together complete the approach to information sharing for the organisation.

Policy makers recognise the importance of expanding the ISG to all vulnerable people in the community not just children, thus the ISG also covers at risk adults such as those with at risk of harm or homelessness, with a disability, frail aged or mental illness. For this reason, the organisation applies the approach in these guidelines for all service and program users, staff and volunteers, where there is an identified concern for the person's safety and well-being or where there may be a risk to public health or safety.

The Appendix includes:

- procedure for gaining consent and discussing limited confidentiality;
- specific guidance for volunteers;
- positions involved in using the ISG and lines of approval/supervision;
- cultural guidance;

- record keeping;
- example case studies (scenarios staff may come across in their work), and
- where to obtain additional advice and assistance.

Procedure for gaining consent and discussing limited confidentiality.

5.1 Seeking consent for the sharing of confidential information is standard practice with all TBCC Inc. service recipients and program users and staff. Service Recipient consent to share their information should be sought whenever it is safe and possible to do so. Informed consent is best provided in writing – for example the consent for a referral to another service provider, however it can be gained verbally, but must be documented in the service recipient, staff or program file (whichever is most relevant to the program or service – and maintained confidentially).

5.2 The key elements to consent are:

- Consent must be provided voluntarily - without threat, pressure or attempting to overpower someone's will.
- The person must be adequately informed of the implications of granting or refusing consent.
- The person must have the capacity to understand, provide and communicate their consent.
- Careful consideration should be given to the appropriateness of obtaining consent (preferably in writing); it must be safe to do so.
- Consent is a process in which:
 - The person is told (or receives information in some other way) about the possible risks and benefits of their information being shared.
 - The person has the chance to ask questions and get them answered to their satisfaction.
 - The person has the opportunity to discuss with family or support people.
 - The person is able to use advice and information to help make a decision that they think is in their best interest.
 - The person communicates their decision to the staff member seeking their consent.
 - The person understands that depending on circumstances, their information may have to be shared with or without their consent, if staff believe sharing will help mitigate risk, may improve their safety and well-being by bringing together better coordinated services, (as per the ISG and 1993 Children's Protection Act) or where there may be a risk to public health or safety.
- Competence and authority may not only be about age or intellectual capacity or mental health – it may also be influenced by literacy, numeracy or cultural factors, some strategies and questions that may help determine this are:
 - Talk through information sharing and its implications at length.
 - Can the person demonstrate their understanding by discussing the implications?
 - Can the person tell you what it means for them?
 - Are there cultural barriers you need to consider, for example the person may be competent but culturally not have the "authority" to provide consent? Is there something you don't know that prevents them from giving consent?

5.3 On rare occasions information may need to be shared without consent in order to prevent causing or escalating serious threats to an individual's well-being or where there is a risk to public safety. This is the limit of confidentiality the organisation can provide and it is important that in obtaining consent for information, this limited confidentiality is made clear. The organisation does this by providing advice on information sharing procedures, to all service recipients, staff and volunteers including children, young people, parents and adults when they enrol in a TBCC Inc. activity/ program. Staff will also revisit an individual's understanding of the consent they have given if the nature of the original consent alters, or if there has been a considerable lapse of time between gaining consent and taking action.

- 5.4 TBCC Inc. will use a general statement about the use of the ISG for inclusion on forms or to be provided to service recipients and staff to advise them about the organisations approach to information sharing.

The statement will read:

TBCC Inc. follows the SA Government Information Sharing Guidelines. This means that this organisation will work closely with other agencies to coordinate the best support for people.

Under the ISG informed consent for the sharing of information will be sought and respected in all situations unless:

- *it is unsafe or impossible to gain consent or consent has been refused and*
- *without information being shared, it is anticipated a child, young person or adult, will be at risk of serious harm, abuse or neglect, or pose a risk to their own or public safety.*

- 5.5 Steps 4, 5 and 6 of the ISG flow chart describe Service Recipient consent (ISG page 19) and see next page. - ISG Decision Making Steps and Practice Guide

5.6 Specific guidance for volunteers

Volunteers support all activities, programs and services of TBCC inc. As part of their role volunteers may have access to information provided by another organisation (eg referrals) and observe the general well being of children, young people and adults.

While volunteers are not authorised to share information with other organisations or government agencies (unless required under mandatory notification in conjunction with their supervisor) they will make an important contribution by advising the CEO when their observations cause them to be concerned about the safety and well being of children, young people or adults.

As part of their induction all volunteers will be made aware of the ISG and who they should report their concerns to.

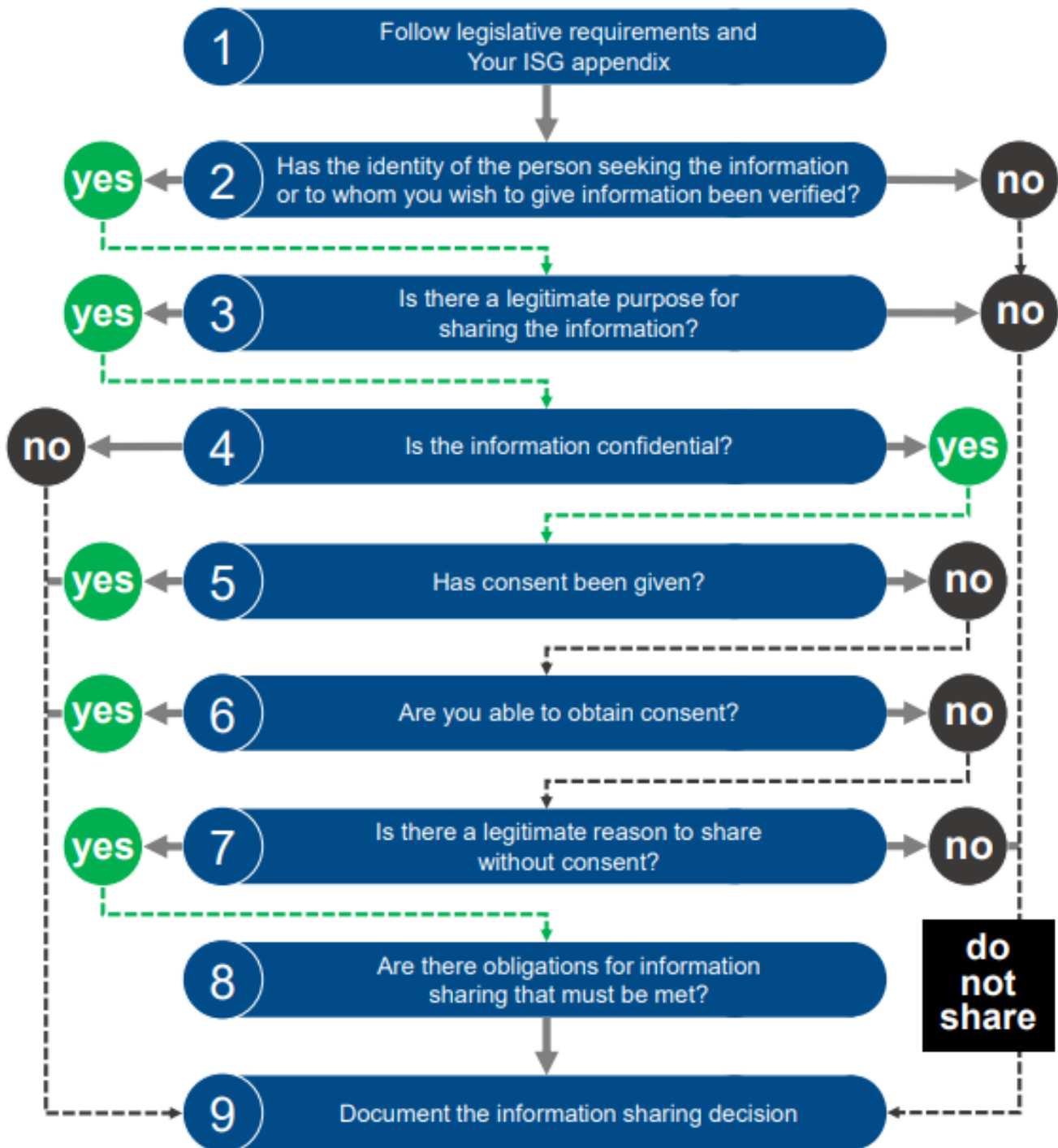
5.7 Positions involved in using the ISG and lines of approval

Most information sharing occurs with the consent of the people concerned. Decisions to share information without consent or refusal to share must be approved by the CEO. The following chart lists those positions that may contribute to information sharing and their specific role.

Positions providing services to children, young people and adults.	Does the role include sharing SR information with other organisations with SR consent?	Is approval required for information sharing without consent or when refusing to share?	Approval from
CEO	Yes	No	
Paid Staff	Yes	Yes	• CEO
Volunteers	No	Yes	• CEO

ISG decision making steps

ISG



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 on (08) 8429 5945 or 1800 952 511 (toll free outside metropolitan South Australia).

- 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.

Date first formulated	12/09/2005	
Dates approved by Board	V1, V2, V3, V4, V5 V6 October 2022	12/09/2005, June 2016, Feb 2018, March 2018, March 2020
Next Review Date	October 2024	
Related Documents	Incident Management System Manual, including Elder Abuse and Serious Incident Response Scheme (SIRS) Policy First Aid Policy Privacy and Confidentiality Policy Information Sharing Guidelines (ISG) Appendix Information Sharing Guidelines (ISG) Consent form Feedback and Complaints Policy Child Safe, and Young Person Wellbeing Policy Child Risk Management Policy Risk Assessment Matrix Risk Management Policy Risk Management Procedure Diversity and Social Inclusion Policy Hot Weather Policy Aged care Charter of rights Aged care Standards Children's Rights National Principles for Child Safe Organisations	
Legislation	Equal Opportunity Act 1984 Work Health & Safety Act Children's Protection Act 1993 Aged Care Act 1997 Privacy Act 1988 Department Human Service DHS Critical Client Incidents Policy Coronial Policy State Records Act 1997 Guardianship Act 1993 Information Sharing Guidelines Australian Human Rights Commission Act 1986 Crimes Act 1914 Criminal Law Consolidation Act 1935 Fair Work Act 2009 Volunteers Protection Act 2001	
Signed on behalf of TBCC Board of Management by:		
Name: Judy Bagg		
Position held: Chairperson		Signature:  5 October 2022