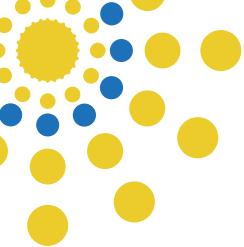


Safe Online Communication with Children and Young People

Practical guidance for organisations





About this guide

This guide builds on the original ***Social Media Communication with Young People factsheet*** developed by Kim Porter. The original resource responded to Australia's social media minimum age requirements and offered practical advice to help organisations communicate safely with young people online.

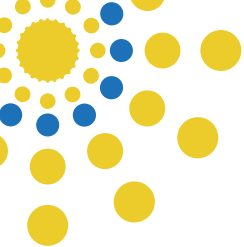
Kooyoora has revised and expanded the resource to reflect changes in the regulatory environment and the many ways organisations connect with children and young people online.

Its scope extends beyond social media to messaging services, email, video calls and education-focused platforms, with guidance on privacy, consent, professional boundaries, platform selection and responses to concerns.

The guide is designed to help organisations make considered decisions about online communication and establish practices that are safe, respectful, transparent and responsive to the needs of children and young people.

Published by Kooyoora

Revised and expanded September 2026



Introduction

Digital platforms can help organisations share information, coordinate activities and support children and young people to participate and stay connected. They can also create risks when communication is private, informal, poorly monitored or conducted through platforms that are not appropriate for a young person's age or circumstances.

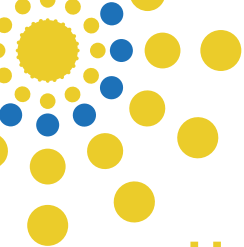
This guide supports organisations to establish safe, respectful and transparent communication practices when using social media, messaging services, email, video calls and education-focused platforms with children and young people.

It draws on:

- Australia's National Principles for Child Safe Organisations
- the Australian social media minimum age requirements
- online safety guidance for child-safe organisations
- privacy guidance for children and young people
- practical tools for implementing the National Principles

The National Principles provide a nationally consistent approach for organisations that engage with children and young people. They emphasise organisational leadership, children's participation, family and community involvement, equity, child-focused responses to concerns, safe online environments and continuous improvement.

This guide provides general guidance. Organisations must also comply with the laws, regulatory requirements and child safety standards that apply in each jurisdiction in which they operate.



Understanding Australia's Social Media Minimum Age Requirements

Australia's social media minimum age requirements took effect on **10 December 2025**.

Age-restricted social media platforms must take reasonable steps to prevent Australians under the age of 16 from creating or maintaining accounts. The responsibility for complying with the law rests with the platforms, not children, parents or carers.

The requirements are intended to reduce young people's exposure to potentially harmful platform features, including recommender systems, infinite feeds, feedback features and disappearing or time-limited content.

Age-restricted platforms

The eSafety Commissioner currently considers the following platforms to be age-restricted:

- Facebook
- Instagram
- Kick
- Reddit
- Snapchat
- Threads
- TikTok
- Twitch
- X
- YouTube



Other platforms may also be covered. The official list is not exhaustive and may change as services, features and regulatory assessments evolve. Organisations should check the eSafety Commissioner's [current list of age-restricted platforms](#) rather than relying on a fixed list.

Under-16s may still be able to view publicly available content that does not require them to log in. However, organisations should not direct young people to social media content without considering the content, platform, privacy implications, accessibility and the child or young person's circumstances.

Services that may not be age-restricted

Certain types of services may be excluded where their sole or primary purpose is:

- messaging, email, voice calls or video calls
- online gaming
- education
- health support
- professional networking or professional development
- sharing information about products or services

However, an exclusion should not be interpreted as confirmation that a service is suitable or safe for organisational communication with children and young people.

Some messaging or other services may fall within the restrictions if they include significant social media-style functions. Platform features and classifications can also change over time.

Organisations should assess each service before approving it and review that decision regularly.



Penalties and responsibility

Children under 16 and their parents or carers are not penalised if a child accesses or maintains an account on an age-restricted platform. The legal obligation rests with the platform.

Platforms that do not take reasonable steps to comply may face significant civil penalties. As penalty amounts can change, organisations should refer to current [Australian Government](#) or [eSafety Commissioner](#) guidance rather than publishing a fixed amount in organisational policies.

Organisations should not:

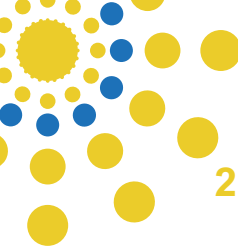
- encourage a child or young person to provide incorrect information about their age
- help a young person bypass a platform's restrictions
- require an under-16 participant to establish an account on an age-restricted platform
- make participation in an activity dependent on access to an age-restricted social media account

Principles for Safe Communication

1. Put children and young people's safety and wellbeing first

Online communication should support the child or young person's participation, safety and wellbeing.

Convenience for the organisation should not be the only reason for selecting a platform or communication method. Organisations should consider whether the communication is necessary, appropriate and proportionate to its purpose.



2. Listen to children and young people

Children and young people should receive clear, age-appropriate information about:

- why the organisation may communicate with them online
- which platforms or channels may be used
- who can contact them
- when communication may occur
- who can view or monitor communication
- what behaviour is expected
- how their information will be used
- how to ask questions, withdraw from optional communication or raise a concern

Their views should inform the selection and review of communication channels. The National Principles for Child Safe Organisations recognise that children and young people should be informed about their rights, involved in decisions that affect them and taken seriously.

3. Involve families, parents and carers appropriately

Parents and carers should be appropriately informed about organisational communication with children and young people.

The nature of this involvement should take account of:

- the young person's age and capacity
- the purpose of the communication
- the nature of the activity or service
- privacy and confidentiality
- the young person's circumstances and safety
- any applicable legal or professional obligations



Parental involvement is important, but it should not be treated as the only safeguard. A parent's presence in a group chat does not replace organisational oversight, clear boundaries, appropriate platform settings or effective reporting arrangements.

4. Use transparent and accountable communication

Communication should ordinarily take place through an organisation-approved channel that can be appropriately supervised, recorded or reviewed.

Staff and volunteers should not use personal social media profiles to connect with children or young people they know through their organisational role.

Where possible:

- use an organisational account or email address
- include more than one authorised adult in group communication
- clearly identify the staff or volunteers responsible for the channel
- maintain appropriate records
- communicate at reasonable times
- keep communication connected to the organisation's activities
- avoid disappearing-message functions
- ensure there is a process for reviewing and responding to concerns

5. Respect privacy

Only collect, use or share the information needed for the communication or activity.



Before approving a platform, consider:

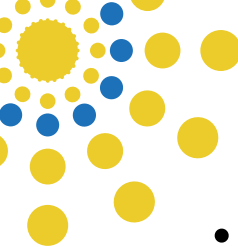
- what personal information it collects
- where information is stored
- who can see participants' names, phone numbers, profile details or images
- whether participants can contact each other privately
- whether the platform uses location data
- whether messages disappear automatically
- whether information can be downloaded, forwarded or captured
- the platform's privacy settings and age requirements
- whether the organisation can manage access when someone leaves
- whether use of the platform is consistent with the organisation's privacy obligations

In Australia, privacy law protects personal information regardless of a person's age. Whether a young person can provide valid consent depends on their capacity to understand what is being proposed. The application of the Privacy Act 1988 can also depend on the type and size of the organisation and the jurisdiction in which it operates.

6. Promote equity, inclusion and accessibility

Communication arrangements should not exclude a child or young person because they:

- do not have a personal device
- do not have reliable internet access
- cannot use a particular platform
- are under the platform's minimum age
- have disability or accessibility requirements

- 
- need information in another language or format
 - have cultural, family or personal circumstances that affect how they communicate

A safe and practical alternative should be available when a child or young person cannot or does not wish to use the organisation's preferred digital channel.

Choosing an Appropriate Communication Platform

Before approving a platform, the organisation should complete a documented risk and privacy assessment.

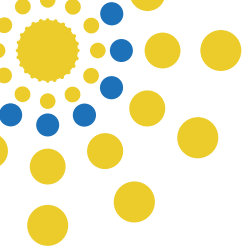
Questions to consider

Purpose

- Why is the platform needed?
- Could the purpose be met through a safer or simpler channel?
- Is communication limited to organisational activities?
- Will the platform support meaningful participation by children and young people?

Age and access

- What is the platform's minimum age?
- Is it age-restricted under applicable legislation?
- Will children need to create personal accounts?
- Could participation pressure a young person to bypass an age restriction?



Privacy

- What information does the platform collect?
- Can participants see each other's phone numbers, email addresses, locations or profiles?
- Are privacy settings controlled by the organisation or individual users?
- Can the organisation remove access when a participant, staff member or volunteer leaves?

Communication features

- Does the platform allow private messaging between participants?
- Does it allow adults to contact children privately?
- Can disappearing messages be disabled?
- Can communication be retained where required?
- Can content be moderated?
- Are there effective block and report functions?

Oversight

- Who will administer and monitor the channel?
- How frequently will it be reviewed?
- Is there a backup administrator?
- How will concerning communication be identified and addressed?
- How will records be preserved when required?



Inclusion

- Is the platform accessible?
- Does every participant have an appropriate way to access it?
- Is there an alternative for participants who cannot use it?
- Have children, young people and families been consulted?

An excluded or education-focused platform should not be described as automatically “safe”. Safety depends on how the platform is configured, managed and used.

Approved Communication Practices

Group communication

Group communication can be appropriate when it is planned, transparent and properly supervised.

Organisations should:

- use an approved organisational account
- have at least two authorised adults able to oversee the channel where practicable
- define who can join the group
- provide children, young people and families with clear participation information
- use settings that limit unnecessary access to personal details
- disable private or disappearing communication where possible
- set expectations for appropriate language and behaviour
- monitor the channel consistently
- remove participants who no longer require access
- retain relevant records in accordance with organisational policy



Including every participant's parent or carer in the same messaging group is not always appropriate. Depending on the platform, this may disclose participants' phone numbers, profile photographs or other personal information. Organisations should consider whether a broadcast list, moderated announcement channel, email distribution list or separate parent communication channel would provide greater privacy.

Email

Email may be suitable for sharing information, announcements and activity arrangements.

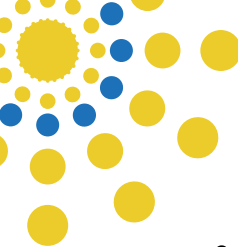
Staff and volunteers should:

- use an organisational email account
- send group emails using privacy-protective address settings, such as BCC where appropriate
- avoid including unnecessary personal information
- copy another authorised adult or organisational account where appropriate
- retain emails in accordance with the organisation's recordkeeping requirements
- avoid using personal email accounts

Video calls

When communicating by video:

- use an organisation-approved platform and account
- schedule the call in advance
- provide clear information about who will attend
- use appropriate privacy and security settings

- 
- avoid recording unless there is a clear purpose, authority and appropriate notice
 - consider whether another authorised adult should attend
 - ensure the setting and conduct are appropriate
 - provide an alternative way to participate where required

Images and recordings

Before capturing or sharing an image, audio recording or video involving a child or young person:

- explain what will be recorded
- explain why it is being recorded
- explain where it may be used or published
- obtain the required consent or authority
- respect the child or young person's views
- avoid including unnecessary identifying information
- confirm whether consent can be withdrawn
- store and dispose of the material securely

Consent to participate in an activity should not automatically be treated as consent to use a child's image publicly.

One-to-One Communication

One-to-one online communication with a child or young person should generally be avoided unless it is necessary for the organisation's work, authorised and managed in accordance with organisational policy.



Where individual communication is required:

- use an approved organisational account
- keep communication connected to the organisation's activities
- communicate at appropriate times
- use clear, respectful and professional language
- maintain appropriate records
- include another authorised adult where suitable
- avoid disappearing-message functions
- do not move the conversation to a personal account
- follow the organisation's procedures if the child raises a concern or asks for support

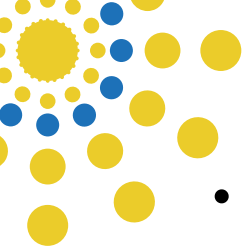
Copying a parent or carer into every message will not be appropriate in every circumstance. The organisation should consider the young person's age, capacity, privacy, circumstances and safety, as well as any legal or professional responsibilities.

Staff and volunteers should never ask a child or young person to keep organisational communication secret.

Boundaries for Staff and Volunteers

Staff and volunteers should not:

- connect with children or young people through personal social media accounts
- use personal messaging accounts unless this is specifically authorised and appropriately managed
- communicate in a way that is personal, secretive or unrelated to the organisation's activities
- use disappearing messages for organisational communication



- share a child or young person's personal information without authority
- post images or recordings without appropriate consent
- communicate at inappropriate times unless there is an authorised and genuine need
- add children to age-restricted platforms
- encourage children to misrepresent their age
- continue private contact after the organisational relationship has ended
- delete communication that should be retained or reported

If a child or young person contacts a staff member or volunteer through a personal account, the adult should move the conversation to an approved channel, preserve any relevant information and follow organisational procedures where the message raises a concern.

Consent and Participation

Consent is one part of safe communication, but it does not replace organisational responsibility.

Organisations should:

- explain the purpose and nature of online communication
- identify the platform that will be used
- explain what information may be visible to others
- explain how communication will be monitored
- advise participants how to leave the channel
- provide an alternative communication option
- record any consent or authority required
- review consent when the platform, purpose or communication arrangements change



Children and young people should also be asked for their views and agreement in a way they can understand. A parent or carer's consent should not be used to override a young person's clearly expressed concern about participating in an optional communication channel.

Monitoring and Recordkeeping

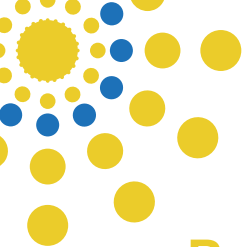
Monitoring should be purposeful, proportionate and clearly explained.

The organisation should determine:

- who is responsible for each communication channel
- how frequently communication will be reviewed
- what records must be retained
- how long records will be kept
- how inappropriate communication will be addressed
- how access will be removed
- who will act when the usual administrator is unavailable
- how monitoring respects children's privacy and participation rights

Monitoring should not create an expectation that every message will be seen immediately. Children and young people should be told that online communication channels are not emergency services and be given appropriate contact information for urgent matters.

The organisation should regularly review its approved platform register, privacy settings, administrator access and communication practices.



Responding to Concerns

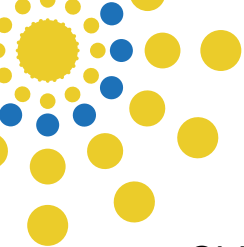
Children and young people should have clear, accessible and age-appropriate ways to report concerning online behaviour.

This may include:

- speaking with a trusted staff member or volunteer
- contacting the organisation's child safety or safeguarding contact
- using an online or written complaints process
- reporting content through the platform
- contacting an appropriate external service or authority

When a concern is raised, the organisation should:

1. Listen carefully and respond without blame or judgement
2. Take immediate steps to address any urgent safety needs
3. Preserve relevant messages, images, usernames, dates and account details
4. Avoid unnecessarily forwarding or reproducing concerning material
5. Follow the organisation's incident, complaint and reporting procedures
6. Notify relevant external authorities where required
7. Explain what will happen next in a way the child or young person can understand
8. Provide appropriate support
9. Protect privacy while sharing information necessary to respond
10. Review whether organisational systems or practices need to change



Children and young people who experience online harm commonly want adults to listen without shaming them, believe their account, help remove harmful content and support them to access further assistance. The [eSafety Commissioner's guidance for child-safe communities](#) provides information about recognising online harm, responding to concerns and helping a child report online abuse.

Using Google Classroom and Other Education-Focused Platforms

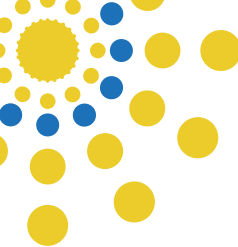
Education-focused platforms may provide useful tools for announcements, resource sharing and structured group activities. However, exclusion from social media minimum age requirements does not mean a platform is automatically safe, private or appropriate for every organisation.

Google Classroom

Google Classroom may be suitable where its features, account arrangements, permissions, privacy settings and data-handling practices have been assessed and approved by the organisation.

Before using Google Classroom, confirm:

- which type of Google account participants will use
- whether the organisation can administer the accounts
- which communication features are enabled
- whether students can communicate privately
- who can post or comment
- whether guardian email summaries are available

- 
- who can access participant information
 - how records will be managed
 - how access will be removed
 - whether use complies with applicable privacy and data protection requirements

Guardian access

Guardians generally cannot sign in to a student's classroom or directly view the Stream, People or Grades pages.

Where the relevant features are enabled, guardians may receive email summaries about matters such as upcoming work, missing work and class activity. Guardian summaries are generally available only when the student is using Classroom through an eligible Google Workspace account. Some education licences provide limited read-only preview links to classwork. More information is available through [Google Classroom Help](#).

Organisations should therefore not tell families that adding a guardian gives them full access to monitor their child's activity.

Safe use of education-focused platforms

Organisations should:

- use organisation-managed accounts where possible
- restrict posting and commenting permissions appropriately
- explain the platform's purpose and rules
- avoid unnecessary collection of personal information
- review participant access regularly
- monitor communication consistently

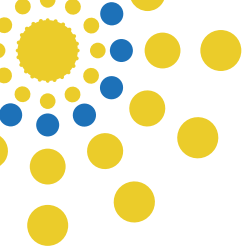


- provide an alternative for participants who cannot use the platform
- train staff and volunteers before they administer the platform
- ensure children and young people know how to report a concern

Communication Plan Checklist

Before communicating online with children and young people, confirm that:

- The communication has a clear organisational purpose.
- The platform has been approved following a risk and privacy assessment.
- The platform is appropriate for the participants' ages.
- Use of the platform complies with current minimum age requirements.
- Children and young people have received clear, age-appropriate information.
- Parents and carers have been appropriately informed.
- Required consent or authority has been obtained.
- An alternative communication method is available.
- Organisational rather than personal accounts are being used.
- Roles for administration and monitoring are documented.
- At least two authorised adults can oversee group communication where practicable.
- Private and disappearing-message functions have been restricted where possible.
- Privacy settings have been reviewed.
- Participants understand the expected standards of behaviour.
- Children and young people know how to raise a concern.
- Recordkeeping and retention arrangements are in place.
- Access can be removed promptly when no longer required.
- The communication arrangement has a scheduled review date.



Template: Information and Consent for Online Communication

These templates can be adapted to suit your organisation's policies, activities and legal requirements.

Purpose:

To provide clear information and record consent or authority where required.

Dear **[parent, carer or guardian name]**,

[Organisation name] uses online communication to share information about **[program, activity or service]**.

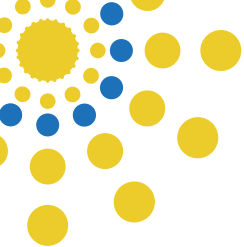
We propose to use **[platform or communication channel]** for:

- **[describe the purpose of communication]**
- **[describe the type of information that will be shared]**
- **[identify who will administer or monitor the channel]**

The platform may make the following information visible to other participants:

[describe names, email addresses, phone numbers, profile information or other details that may be visible]

Communication will be managed in accordance with our **[Child Safety and Wellbeing Policy, Code of Conduct, Privacy Policy and Communication Policy]**.



Participation in this communication channel **[is/is not]** required. The following alternative is available:

[describe the alternative communication method]

If you or your child has a question or concern, please contact:

Name:

Position:

Contact details:

Participant details

Child or young person's name:

Program or activity:

Preferred communication method:

Accessibility or communication requirements:

Consent or authority

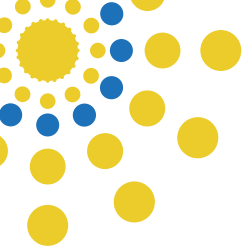
Please select one:

- ☐ I consent to the child or young person named above participating in communication through **[platform]**.
- ☐ I do not consent to participation through this platform and would like to use the alternative communication method.
- ☐ I would like further information before deciding.

Parent, carer or guardian name:

Signature:

Date:



Child or young person's agreement

I have received information about how the communication channel will be used and who I can speak with if I have a question or concern.

Child or young person's name:

Signature or other indication of agreement, where appropriate:

Date:

Template: Online Communication Incident Record

Date and time of incident:

Platform or communication channel:

People involved or affected, where relevant:

Person recording the incident:

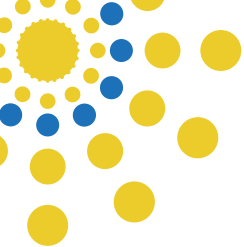
Description of what occurred:

Immediate safety concerns identified:

Immediate action taken:

Relevant information preserved:

- ☐ Messages
- ☐ Account or profile details
- ☐ Dates and times
- ☐ Screenshots
- ☐ Links or URLs
- ☐ Other relevant records



Child or young person's views and support needs:

Parent or carer notified, where appropriate:

Internal person notified:

External report or referral made:

Further action required:

Person responsible for follow-up:

Review date:

Outcome and actions taken to prevent recurrence:

Incident records should be stored securely and shared only with people who require the information to respond appropriately.

Scenario 1: Coordinating a Youth Activity

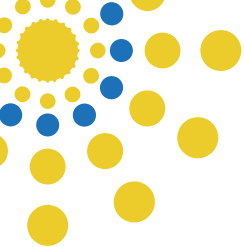
Situation

An organisation needs to communicate schedule changes and reminders to young people attending a weekly activity.

Safer approach

The organisation assesses available options and establishes a moderated announcement channel using an approved organisational account. Two authorised adults can administer the channel.

Participants cannot contact one another privately through the channel, and an email option is available for families who do not use the platform.



Young people and families receive information explaining:

- the purpose of the channel
- who administers it
- what information will be shared
- expected behaviour
- how to raise a concern
- the alternative communication option

Why this approach is safer

The arrangement supports participation while reducing private communication, unnecessary disclosure of personal information and reliance on one adult.

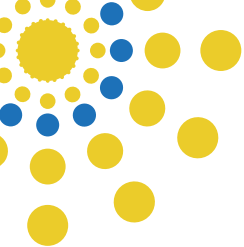
Scenario 2: A Young Person Sends a Private Message

Situation

A young person sends a staff member a direct message through the staff member's personal social media account about an organisational activity.

Safer approach

The staff member does not continue the conversation through the personal account. They preserve the message if necessary, respond briefly with the approved organisational contact details and move any further communication to an authorised channel.



If the message raises a concern about safety or wellbeing, the staff member follows the organisation's reporting and response procedures rather than simply redirecting it.

Why this approach is safer

The response maintains professional boundaries without ignoring the young person or creating an obstacle to raising a concern.

Scenario 3: Moving Away from an Age-Restricted Platform

Situation

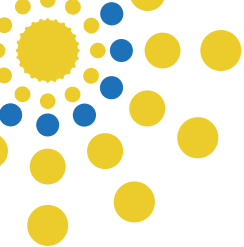
A group previously used an age-restricted social media platform to provide updates to participants under 16.

Safer approach

The organisation consults participants and families, assesses alternative platforms and selects an age-appropriate channel that does not require an under-16 participant to hold an age-restricted account.

It provides:

- clear transition instructions
- an alternative for participants without suitable digital access
- updated privacy and participation information
- a contact person for questions
- training for the staff and volunteers who will manage the new channel



Why this approach is safer

The organisation meets its responsibilities without encouraging young people to misrepresent their age or lose access to important activity information.

Scenario 4: Choosing a Group Messaging Service

Situation

An organisation is considering a messaging group that would display every participant's phone number and profile details to all other group members.

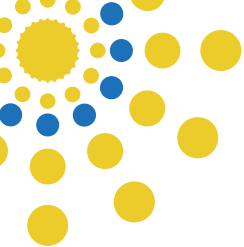
Safer approach

Before creating the group, the organisation considers whether an announcement channel, broadcast function, organisational email list or separate communication channel for parents and carers would meet the same purpose with less disclosure of personal information.

If the messaging group is approved, participants receive clear information about what details will be visible, privacy settings are reviewed, and an alternative communication method is offered.

Why this approach is safer

The organisation considers privacy and data minimisation rather than assuming that a group message is safe simply because several adults are included.



Reviewing Organisational Practice

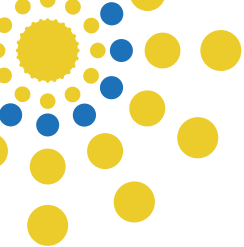
Online platforms, laws and patterns of use change quickly. Organisations should review their communication arrangements regularly and whenever:

- a platform introduces new features
- a platform changes its age requirements
- legislation or regulatory guidance changes
- a new platform is proposed
- a concern or incident occurs
- children, young people or families identify a problem
- the organisation's programs or participant groups change
- monitoring identifies that policies are not being followed

The review should include the views of children and young people, families, staff and volunteers.

Organisations should maintain an approved platform register recording:

- the name of the platform
- its approved purpose
- the age group for which it is approved
- its main privacy and safety risks
- required settings and safeguards
- the responsible administrator
- the approval date
- the next review date



How Kooyoora can help

Safe online communication requires more than choosing the right platform. Organisations also need clear policies, appropriate boundaries, effective oversight and staff and volunteers who understand their responsibilities.

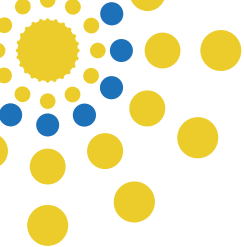
Kooyoora works alongside organisations to strengthen their approach to online communication with children and young people. Kooyoora can help with:

- developing and reviewing policies, procedures and codes of conduct for online communication
- identifying and managing risks associated with social media, messaging services, email, video calls and online platforms
- training staff and volunteers to communicate safely and maintain appropriate professional boundaries
- strengthening complaints, reporting and incident response processes
- reviewing broader organisational systems and practices that support child safety
- complaints management and independent investigations when concerns arise

Preventing harm through culture change

Safe online communication starts with a culture where expectations are clear and children and young people feel heard and supported. Kooyoora's Abuse Prevention Through Culture Change Framework provides free, research-informed tools to help organisations identify risks and strengthen their culture.

[Explore Kooyoora's Safeguarding Services](#)



Additional Resources

- National Office for Child Safety: National Principles for Child Safe Organisations
- Australian Human Rights Commission: Child Safe Organisations implementation tools
- eSafety Commissioner: Social media age restrictions
- eSafety Commissioner: Guidance for child-safe community organisations
- Office of the Australian Information Commissioner: Privacy guidance for children and young people