



Contextual safeguarding of children and teens online:

a guide for child and family sector professionals

September 2026

About this guide

The guide provides a practical framework to help professionals in the child and family sector identify and respond to online risks for the children, teenagers and families they support. It is designed to complement your organisation, service or practice's existing safeguarding policies and procedures, and to ensure children's online lives are considered as part of safeguarding.

It outlines key actions for ensuring the online lives of children including teenagers are fully considered when safeguarding against the risks and issues they may face. It also includes activities you can use with children including teenagers. You might use this guide in initial assessment meetings, during regular check-ins, or as part of children, youth or family events. Organisations, services and practices can also use this guide in staff development activities and to inform policies and procedures.

The guide uses trauma-informed approaches that recognise the importance of safety, trust, choice, collaboration, empowerment and avoiding blame. Responses to online harm should seek to minimise shame and support recovery.



Contents

Contextual safeguarding – an explanation	4
Identify risks	7
• Mapping activity for children	10
• Mapping activity for teens	11
Policies and procedures	12
Relationships and partners	14
Action plans and safer outcomes	15
Case study	17
Checklist	19
About eSafety	20
References and further information	21

How we talk about children and families

Throughout eSafety's website and resources we use 'families' and 'parents and carers' to talk about the adults who support children. When we use these terms, we include the mums, dads, parents, carers, aunties, uncles and other supportive adults who we know can have an important role in helping children play, learn and grow.

When we talk about 'children' we mean everyone under 18 years old. Sometimes we include the term 'young people' because many teenagers don't like to be called children.



Contextual safeguarding – an explanation

Contextual safeguarding looks at how we can best understand and prevent risks to help keep children safe. It is an approach to protecting children from harm occurring outside the family home – such as in schools, communities, employment, online and from peers – where parents and carers may have limited control.

It places the child at the centre, recognising that their safety and wellbeing is influenced by the environments and relationships around them. It shifts the focus from considering only individual or family vulnerabilities toward assessing and intervening in other environments and situations where abuse may also happen.

Contextual safeguarding supports professionals to develop a greater understanding about the lives and experiences of children, to support the prevention of serious harms including child sexual abuse online. It complements other theoretical approaches to child safety that may be used in organisation, services or practices including social ecological model approaches. These approaches can be used with children living in the family home or alternative care arrangements.

Considering online harms and risks as part of contextual safeguarding

Contextual safeguarding includes the consideration of safe and effective online practices for children, families, and staff in policies, procedures, and infrastructure within your organisation, service or practice. Policies, procedures and infrastructure should:

- assess online safety risks and define strategies for addressing them (see esafety.gov.au/communities/child-safe-communities/risks)
- include procedures for reporting online abuse
- uphold the digital rights of children and the **National Principles for Child Safe Organisations** (see Resource hub in humanrights.gov.au), including balancing the right to safety, freedom and protection online, as well as centring the needs of the child.

This guide identifies four actions child and family sector professionals can use to support children to participate safely and confidently online:

- **Identify** the online environments, for example: platforms, apps, and websites where harm could occur – and the risks children face on them.
- Consider the **policies and procedures** in your organisation, service or practice that can influence how you safeguard children online.
- Establish and build on **relationships and partnerships** that have a reach into environments where harm can occur.
- Use an **action plan** to decide specific strategies to mitigate risks.

How does contextual safeguarding support better online safety?

As children explore, play and connect with others online, they can face risks.

Online harms include (for more information esafety.gov.au/key-topics):

- exposure to distressing or harmful content
- contact by an adult (known or unknown to them) who intends to harm them – for example through sexual abuse, cyberflashing, cyberstalking, identity theft or recruitment to extremist groups
- experiencing, or seeing or participating in harmful behaviour such as cyberbullying, trolling or sexual harassment or becoming involved in dangerous trends or user communities (for example, encouraging unsafe challenges, self-harm or eating disorders)
- exploitation by potentially harmful commercial operations such as scams, gambling and exploitative or age-inappropriate marketing. (It also includes illegal trading that impacts a child, such as using the internet to distribute sexual exploitation material of them)
- child sexual abuse, including grooming and sexual extortion (sometimes called ‘sextortion’).



Unlike a single incident of physical harm, online abuse can spread rapidly without a clear end point. Children who are victim-survivors describe living with the ongoing possibility that abusive content, including child sexual abuse material, could resurface or be re-shared at any time.

Child and family sector professionals need to be engaged and informed about the harms faced by children, both offline and online, and the strategies they can employ to reduce the risks.

Contextual safeguarding looks beyond the individual child to identify:

- who may be influencing them (both positively and negatively)
- the degree of that influence
- what strategies can be employed with the child to reduce risks.

This includes looking at what children are doing online and where, including on social media, gaming platforms, messaging apps, community forums and in collaboration spaces for education and work. It also considers who children are interacting with while in these spaces.

Contextual safeguarding against online harm comprises prevention efforts that target factors external to the individual child, addressing **safety and response** planning to create safer environments for children.

- **Safety planning** can consider peer groups, safe and trusted adults, social and recreational settings and online spaces. For older children consider the school or workplace as settings in which abuse can happen offline and online.
- **Response planning** can include strategic partnerships, inter-agency working and community engagement, as well as challenging societal attitudes that normalise sexual abuse including grooming, or violent behaviour.

eSafety provides a reflection and planning tool ([see esafety.gov.au/communities/child-safe-communities/tool](https://esafety.gov.au/communities/child-safe-communities/tool)) that helps child and family sector professionals, organisations, services and practices assess risks and plan a holistic approach to online safety.

The questions in the tool can guide a review of strategies for preventing, recognising and dealing with online abuse. They will also suggest ways to reduce stigma and empower communities to take safeguarding action.

Identify risks

Digital devices and technologies, including online platforms and services, have many benefits. They can help us find connection, support and information and enable us to collaborate, socialise, learn and work. But they come with risks, especially for children including teenagers.

Contextual safeguarding needs to begin with an investigation of the risks and protective factors within the online environments frequented by children. This helps to build an understanding of the factors in those settings that might contribute to abuse and help with its prevention, as well as develop a plan with a child to reduce the likelihood of online abuse happening.

Early detection prevents escalation and knowing what support to provide when harm does occur helps minimise the impacts. For example, changes in a child's online activity may signal wider concerns, including grooming or exploitation, harmful peer influence, declining mental health, placement stress, absconding risk, or contact with unsafe people.

Changes to look out for include the child suddenly avoiding favourite apps or platforms, becoming secretive about device use, or appearing worried, uncomfortable or upset after being online.

Online abuse can happen on a social media site, game, app, or any other online or digital service or platform. It can include posts, comments, texts, messages, chats, livestreams, memes, images, videos and emails. AI-generated images or videos can also cause real emotional, social and reputational harm.

It is important to recognise that while children with diverse needs and circumstances may rely more heavily on online spaces to participate equally and find support for their identity and wellbeing, they may also be more vulnerable to abuse. This includes online spaces creating opportunities to target children and teenagers because of their race, sex, gender identity, sexual orientation or disability. Younger children and those with diverse needs, particularly children with disability, may experience additional barriers to telling safe and trusted adults when harm has occurred.

Note that online abuse can have harmful mental and physical impacts. In addition, online abuse such as bullying or sexual abuse, is often an extension of – or can lead to – offline abuse.

To help you identify risks, it is useful to map a child's interactions with online environments and assess how safe or unsafe they feel in those spaces. This will help identify where it's best to focus your efforts.

Mapping the child's online world

Mapping activity templates included in this guide are designed for children aged 5 to 12 and 13 to 18.

Sit down with the child you are supporting and talk with them about the platforms, apps, websites, forums and other online spaces that they regularly use or visit. This includes AI-powered platforms such as companions, chatbots and image generators. Consider what devices they have access to and any parental controls or safety settings currently in place for those devices.

Starting with a relaxed conversation and approaching their online world with curiosity can help you build trust, which will be important when discussing more challenging topics such as online risks and harms. It can be helpful to acknowledge to children that adults do not always know the platforms or apps they might be using and that we are not trying to catch them out or take their devices away from them. Make sure they understand that they will not be in trouble or penalised if they are on a platform or app that they should not be using (such as social media if they are under 16 or online pornography if they are under 18). Be honest and open that you are trying to keep them safe and be genuinely curious about their online world. You can say things like:

- How did you find out about {online space}? Why did you want to explore it?
- I haven't seen {online space} before. I'd like to know a bit more about it. What do you like about it? Dislike?
- I talk to lots of children and they enjoy using {online space} for lots of different reasons. Why do you use it?
- Who are the important people in your online world? Are they people you know in person?
- Are there communities or groups you're part of online? How do you participate in the group?
- Is there anyone you wish understood more about your online life? What would you like them to know or ask you?

Once you have mapped the online environment, using a copy of the visual map in this guide, have the child indicate the spaces where they feel safe and where they may feel less safe at times – you can use stickers or coloured pens to mark safe, unsafe or unsure.

You can also consider at this stage if there are any offline factors that might make an online space feel unsafe, for example bullying at school that is carrying over into an online environment.

Explore with the child why an online space might feel safe or unsafe, and the potential risks in a space that need to be considered. You could use conversation prompts like these. You may wish to adjust them to be age or developmentally appropriate.

- What do you use {online space} for? Do your friends use {online space} as well?
- What is it about {online space} that makes you feel safe? Has it always felt safe?
- How do you know if an online space is unsafe?
- Are you able to share an example of an online space that made you feel unsafe?
- What kind of things do you do to keep yourself safe on {online space}?

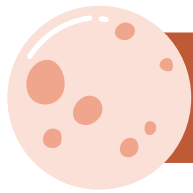
eSafety has conversation cards that can help you start the conversation (see esafety.gov.au/parents/issues-and-advice/protecting-children-from-sexual-abuse-online/resources).

It is important to remember that while a child might feel safe in a particular space, or the platform may be popular among their peers, there may be inherent or unknown risks that need to be considered as part of this conversation. **The eSafety Guide** (esafety.gov.au/key-topics/esafety-guide) can help you assess the risks that a child might be exposed to on a variety of platforms, apps and websites.

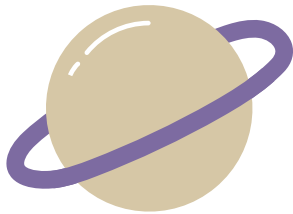
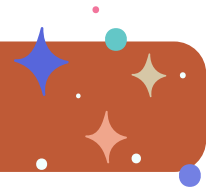
Online harms often do not occur as isolated incidents. Consider whether any concerns form part of a broader pattern across time, settings or relationships. It may be useful to return to the mapping exercise regularly to consider any changes to the child's online activities or relationships. For example, you can talk about these topics.

- Emerging concerns
- Patterns of online contact
- Escalating behaviour
- Shifts in the child's feelings of safety or risk





My online space







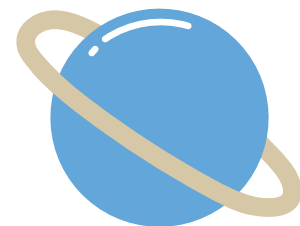


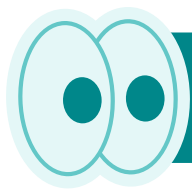








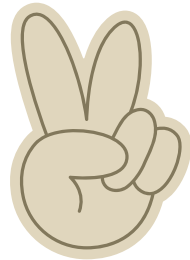


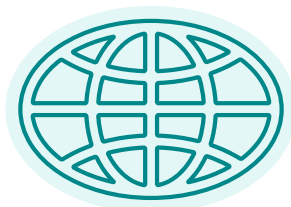


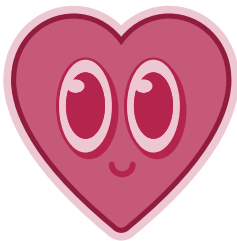
My online space

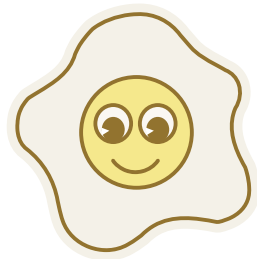






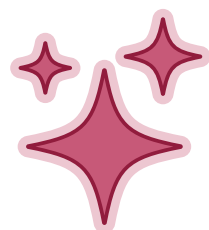












Policies and procedures

Supporting online safety for children is a shared responsibility. It requires a holistic approach that integrates best practices and legal requirements, fosters supportive and collaborative relationships, and strengthens organisational systems to ensure safety, empowerment, and online participation.

As part of the contextual safeguarding of a child or young person you are supporting, it is important to also consider any legal or regulatory requirements you may have to follow as well as your organisation, service or practice's policies on child safeguarding. (For more, see esafety.gov.au/communities/child-safe-communities)

As well as the efforts of individuals, organisations have a responsibility to consider environmental risks and implement system-level responses when harms are identified. Organisations should ensure online safeguarding risks are incorporated into governance, risk management frameworks, staff supervision, incident review processes, training programs and continuous improvement activities. Clear accountability should exist for prevention, reporting, response, review and follow-up. The National Principles for Child Safe Organisations (childsafety.gov.au/resources/national-principles-child-safe-organisations) emphasise the importance of physical and online environments that promote safety and wellbeing while minimising the opportunity for children and young people to be harmed (Principle 8).

Technological platforms within organisations, whether publicly available or in-house, provide valuable tools for education, communication and help seeking. Risks associated with these platforms should be minimised through all available means, including the application of safety filters and the education of children, parents, staff and volunteers about expectations of online behaviour and communication protocols.

Your organisation, service or practice should have policies and protocols for communicating with children including teenagers, especially if you are familiar with them in both a professional and personal capacity where boundaries can be blurred. This protects both you and the child.

Make sure you are familiar with any mandatory reporting requirements that might relate to your role if you suspect child abuse is occurring. You should also be familiar with the laws that govern online activities, including laws that make it illegal to groom children for the purpose of sexual abuse or to create sexual abuse and exploitation material.

Child and family sector professionals play a crucial role in helping to mitigate risks by:

- following their organisation, service or practice's policies and procedures, and ensuring they are clearly communicated to families
- being proactive in identifying potential dangers and mitigating the online risks that children may be exposed to
- helping children build the skills to engage more safely online, including how to report unsafe situations
- providing support to children when harm occurs
- helping children build resilience and confidence to manage online challenges
- letting children know they can talk to you if they feel unsure, uncomfortable or unsafe online
- providing education (esafety.gov.au/communities/child-safe-communities/families) to children, their families, communities and other services about online safety and action that can be taken – for example reporting online harms to police and/or eSafety (esafety.gov.au/report)
- staying up to date (esafety.gov.au/newsroom) with new developments and environments online that could contribute to risk and harm to children
- ensuring children understand their rights and know how to make a complaint or raise concerns about any of the conversations or activities taking place.



Online child sexual exploitation, including online grooming and sexual extortion, should be reported to the Australian Federal Police-led **Australian Centre to Counter Child Exploitation** (ACCCE accce.gov.au).

Reports can also be made in confidence to Crime Stoppers on 1800 333 000 or at crimestoppers.com.au.

Anyone can report (esafety.gov.au/report) online child sexual exploitation and abuse material to eSafety at any time, so we can have it removed. Your report can be anonymous.

Anyone whose nude or sexual image or video has been shared online without their consent can report it to eSafety (esafety.gov.au/report), so we can have it removed.

Relationships and partners

Some children are supported across multiple households, services, carers, staff teams or agencies. In these circumstances, online safety planning should clarify roles, information sharing arrangements, consistency of expectations and who will support the child before, during and after any online safety concern. Treating safeguarding as ‘everyone’s responsibility’ means the safe and trusted people in a child’s life are partners in creating safe spaces, identifying risks and harms, and reporting or sharing information about those risks and harms. This means an active role can be played by individuals, organisations, services, practices, workplaces, schools or anyone else in contact with children.

Where possible, it can be helpful to establish communication and information sharing between the various professionals involved in a child’s wellbeing to align safety approaches and goals. These connections can be formal or informal. Keep in mind appropriate measures, including your organisation’s policies around protecting the child’s right to privacy.

When information is being shared, it is helpful for children to understand what is being shared, with whom, and why. Consider what the child may need to know to help maintain their trust, taking into account their age and stage of development.

Families often have valuable knowledge about a child’s online experiences, interests, friendships and behaviour that may not be visible to professionals. Equally, professionals can help families understand emerging online risks and protective strategies. Strong relationships and open communication between parents, carers, child and family sector professionals, educators and student wellbeing support staff, and other key adults in the child’s life can help to identify issues early and prevent them escalating. This includes:

- sharing information appropriately
- clear and consistent messaging
- coordinated safety planning.

It is often best to involve the child’s family in online safety planning where possible. eSafety provides advice for professionals supporting families with online safety at esafety.gov.au/communities/child-safe-communities/families.

Children's significant relationships include friends and peers – in addition to the relationships they have with extended family members, online communities and in workplaces. Think about who in the child's life they spend time with. Do they have a role to play in supporting children in addition to their parent or carer? These relationships can be important in safeguarding if the first safe and trusted adults a child discloses online harm to are unable or unwilling to help.

When developing strategies with the child to keep them safe online, consider the role each of these potential partners could play. This can include creating formal agreements within care teams through to talking with the child about how their friends support them if something happens online. The child themselves is also a partner in this and they may have strategies they are already using or have insight into what works best for their situation that must be considered.

Action plans and safer outcomes

It is time to create a plan of action, now that you have considered any legal or policy requirements around online safety, defined the child's online world (including where they feel safe or unsafe) and identified partners to help keep them safer online.

eSafety has a range of resources that you can use with children to develop preventative online safety strategies that work for them. These include:

- family tech agreements (esafety.gov.au/parents/resources/family-tech-agreement)
- tech safety plans (esafety.gov.au/key-topics/domestic-family-violence/support-service-resources/supporting-kids-dealing-with-tech-abuse/my-tech-safety-plan)

Children, including teenagers, often have their own unique ways of perceiving safety that may not always be acknowledged by adults. They also have varying levels of digital literacy compared to adults. It's important that children continue to build their digital literacy skills such as recognising signs of scams, privacy risks and the influence of algorithms on what they see and interact with.

As part of developing the action plan, agree to and establish some boundaries related to where children use devices, the time of day, the amount of time they spend on them and the online activities they do. You should also outline how parents, carers, friends and other trusted adults might use protective actions to keep the child safe, including children's rights to privacy and the protection of their identifiable images. eSafety has some information on online safety basics and privacy to help families get started.

(See esafety.gov.au/parents/issues-and-advice)

Parental controls (esafety.gov.au/parents/issues-and-advice/parental-controls) can be used to support a child's online safety but it is important for families to understand their limitations and use them in combination with other protective strategies – conversations about their use and online safety being one of the most effective. In some cases, parental controls can be misused.

When developing these plans encourage the child to consider:

- What makes you feel safe online?
- What can I do to feel safe online?
- What can others do to keep me safe online?
- What will I do if I feel unsafe online?

It is important that children feel confident telling a trusted adult when something doesn't feel right, especially when they are online. Talking with the child regularly – and calmly – about what they do online and what to do if something makes them feel unsure, uncomfortable or unsafe online, helps children feel safe to come to their trusted adults when they need help.

If harm has occurred, it can help to build and maintain trust to ask the child what they would like to happen next, and work with them to meet their requests where possible and appropriate. It can also be helpful to support children to find alternative activities if their current preferences are not safe. It's also important to support children's safe and developmentally appropriate use of technology, as well as their skills in recognising unsafe situations, and practice simple safety rules.

Remember to regularly review the plan with the child so that it continues to reflect their current situation, age and development. It can be helpful for families to revisit any conversations and agreements when introducing children to new devices, platforms, or apps.



Case Study – Responding to inappropriate online conduct in residential care

Kelly is 14 and uses overnight respite care for three nights per week in a staffed residential home.

A youth worker, Marcus, observed that Kelly was spending increased time on a popular online world-building game that included an open chat function. Kelly appeared withdrawn and protective of her device. Noticing this, Marcus created a safe space to check in with her.

He gently said 'I've noticed you seem a bit quieter today. If something online is bothering you, you can tell me.'

Kelly shared that another user had been sending inappropriately sexual messages and demands for photos, and that the interaction had made her feel unsafe and uncomfortable.

Marcus responded calmly, 'Thank you for telling me. You've done the right thing.'

He reassured Kelly, 'You are not in trouble, and this is not your fault.'

Marcus validated her feelings, saying 'It makes sense that you'd feel uncomfortable'.

Marcus immediately notified his manager and followed organisational child safe procedures. Marcus and Kelly talked, using age-appropriate language, about the steps that would be taken to keep her safe.

Marcus explained, 'Because this involves your safety, I need to follow our reporting process. We'll go through this together, and I'll stay with you.'

In line with reporting requirements, the incident was documented and local police and the Australian Centre to Counter Child Exploitation were notified. Marcus and his manager met with Kelly's family to let them know about the incident and to discuss the steps agreed with Kelly to keep her safe online. Other residential staff, Kelly's teachers and school principal were also briefed, and a follow-up meeting with her family was scheduled to ensure consistent supervision strategies and online safety support across the family home, school and respite setting.

Kelly contributed to the development of a safety plan. She was involved in deciding to disable the open chat function in the game, restrict communication to known contacts, and report and block the other user. The conversation also focused on building her digital literacy (see esafety.gov.au/parents/issues-and-advice/online-safety-basics) and confidence so that Kelly could continue using technology in a safe and developmentally appropriate way.

In the days following the incident, staff regularly checked in with Kelly and reinforced that she was not responsible for the inappropriate behaviour and that speaking up was a strength. Kelly was offered access to therapeutic support and provided with age-appropriate online safety education from eSafety (esafety.gov.au/young-people) to rebuild confidence. Marcus kept in touch with Kelly's school to ensure the online safety education she received addressed any gaps from when she'd missed school, and aligned with her class curricula. They also discussed Kelly's specific needs so the education remained positive and strengths-based.

(Case study provided by the NSW Office of the Children's Guardian.)



Checklist

Use this checklist to keep track of the contextual safeguarding actions you have taken. You may not need to address every action in every case or follow the same order.

Mapped the child's online world using the templates in this guide

Identified strengths

Identified risks

Identified safe and trusted adults

Reviewed organisational policies

Communicated relevant organisational policies with the child, their family and other professionals

Established clear communication protocols with the child's online safety partners

Spoken with families and/or other safe and trusted adults about the child's online activities and safety

Developed an agreed action plan

Scheduled a review



Report to eSafety



Family tech agreements



Communities hub

About eSafety

eSafety helps Australians to prevent and deal with online harm. (See esafety.gov.au/key-topics)

We can help to remove:

- serious abusive online content (such as cyberbullying of children) if the service or platform does not help
- illegal and restricted online content including child sexual abuse material.

Trusted adults can help make a report to eSafety if a child is experiencing serious online harm, at esafety.gov.au/report.

To get urgent help for child sexual abuse, including grooming and sexual extortion, report what's happened to the Australian Centre to Counter Child Exploitation (ACCCE) at accce.gov.au/report.

You can make it easier for children to ask for help if they have a negative online experience by talking with them about how the platforms and eSafety can assist. To find out how to protect your personal information and report harmful content on common social media, games, apps and sites, you can refer to esafety.gov.au/key-topics/esafety-guide.

eSafety provides a range of resources for parents and carers, to help understand online safety issues and talk with children about them. This includes advice for parents and carers for starting online safety conversations about challenging topics such as child sexual abuse online at esafety.gov.au/parents/issues-and-advice/protecting-children-from-sexual-abuse-online.

For families who wish to upskill their digital and online safety literacy, eSafety regularly delivers free webinars on a range of topics. (esafety.gov.au/parents)

More resources and guidance for child and family sector professionals about safeguarding children online can be found at esafety.gov.au/communities/child-safe-communities. This includes advice and tools so your organisation, service or practice can help prevent and handle online risks and harms, while improving online safety among families in your community.

References and further information

Global Centre for Contextual Safeguarding - [Contextual Safeguarding Research Durham University](#)

Firmin and Lloyd, 2020 [cs-briefing-a-2020-update-on-the-operational-strategic-and-conceptual-framework2020-final.pdf](#)

Institute of Child Protection Studies, Australian Catholic University and Sexual Violence Prevention and Response Unit, University of Sunshine Coast - [Child-safe practices using contextual safeguarding strategies - ACU](#) and [Advancing organisational child-safe practices using contextual safeguarding strategies | UniSC | University of the Sunshine Coast, Queensland, Australia](#)

National Society for the Prevention of Cruelty against Children - [Podcast: An introduction to contextual safeguarding | NSPCC Learning](#)







