Child Safe Organisations
National Principles

Child Safe Organisations: Checklist for online safety

This Checklist will assist organisations to consider potential safeguarding risks and aspects of online safety in order to better protect children and young people.

Why is online safety important?

Online platforms are valuable tools for education and communication. They provide children and young people with a range of opportunities to learn in new and interactive ways, to engage with others, and to seek help and information. Organisations providing services to, or working with, children and young people have a responsibility to ensure that where children participate online they are protected from harm.

The National Principles for Child Safe Organisations recognise the importance of safe physical and online environments to promote the safety and wellbeing of all children and young people.

The checklist below is a starting point to identify when your organisation should take steps to ensure a safe online environment, and how to go about doing this.

Online safety risks that your organisation may have to deal with include:

- The potential for inappropriate relationships between adults in a position of trust and the children and young people they work with
- Online abuse[1], including bullying[2], non-consensual sharing of intimate images[3], image-based abuse[4], online grooming, online exploitation and abuse, or unwanted online contact[5]
- The exposure, or publication and distribution of inappropriate imagery or content[6]
- Data breaches of personal data and information, and data misuse
- The uploading of content[7] by adults or children and young people featuring children and young people without informed consent
- Age-inappropriate access to online content[8].

Developing online safety policies, protocols and procedures – with the involvement of staff and volunteers, children, young people and their families – will help ensure that everyone is informed, better protected, empowered to act, and has the opportunity to receive early help and support when online safety incidents occur.

Informing everyone and encouraging their engagement with these documents shows that your organisation is taking all possible steps to ensure that it is a child safe organisation.

Organisations can find information about the statutory powers of the Office of the eSafety Commissioner on the website[9]. Organisations should be aware of relevant legislation in their jurisdiction. In particular, the *Criminal Code Act 1995* (Cth) (Division 474, Subdivision C) captures a wide range of offences, which have relevance for the online environment.

The checklist

If any of the following apply to your organisation, you should take steps to develop policies and procedures to better protect your members. See the 'More information' section below for further resources that can assist. Does your organisation:

Allow access to the internet on its premises?	YES	NO	N/A
Have a website and/or social media accounts?	YES	NO	N/A
Allow the use of social media, e-mail, instant messages and other digital technologies to communicate with each other, including with children and young people, and with the public?	YES	NO	N/A
Allow the recording of events, the use of personal and/or professional digital devices?	YES	NO	N/A
Store and/or publish photos and videos on the organisation's website or social media accounts?	YES	NO	N/A
Allow children and young people to bring their mobile devices into the organisation?	YES	NO	N/A
Allow photos or videos of children and young people to be taken and published on personal social media accounts, or anywhere online?	YES	NO	N/A
Provide digital devices for use on or outside the organisation's premises?	YES	NO	N/A
Collect personal data?	YES	NO	N/A
Have protocols and procedures in place to deal with online incidents?	YES	NO	N/A

Keeping children and young people safe online

Simple steps can be taken to help children and young people be safe online. These include:

- Teaching everyone in your organisation about online safety issues[10] and about appropriate online behaviour

- Helping everyone understand online risks, how to navigate the online world safely and empowering them to be able to keep themselves safe online
- Clarifying the importance of keeping personal data and information safe and secure[11], and outlining procedures in this regard
- Making it clear that everyone in the organisation is responsible for the online safety of children and young people
- Outlining how the organisation will respond to the misuse of digital devices and to unacceptable online behaviours
- Having clear processes for reporting online safety issues or breaches of acceptable use policies.

Making a plan

To ensure your organisation is child safe, it is important to develop online safety policies and procedures linked to your child safety and wellbeing policy and code of conduct. The steps your organisation will take will depend on the extent of its online engagement. Any steps your organisation takes should align with the relevant state, territory and national legislation and guidance, and may include the areas of acceptable use, the use of social media, and how to respond to incidents and data breaches.

More information

For more information, practical tools and resources on online safety, visit the **Office of the eSafety Commissioner** website at https://www.esafety.gov.au/.

For more information, practical tools and resources on the **National Principles for Child Safe Organisations,** visit the website at https://childsafe.humanrights.gov.au/.

For information on the **National Office for Child Safety,** visit the website at https://pmc.gov.au/child-safety.

1 Office of the eSafety Commissioner, *Cyber abuse*. At https://www.esafety.gov.au/esafety-information/esafety-issues/cyber-abuse
2 Office of the eSafety Commissioner, *Cyberbullying*. At https://www.esafety.gov.au/esafety-information/esafety-issues/cyberbullying
3 Office of the eSafety Commissioner, *Sexting*. At https://www.esafety.gov.au/esafety-information/esafety-issues/sexting
4 Office of the eSafety Commissioner, *Image-based abuse*. At https://www.esafety.gov.au/image-based-abuse
5 Office of the eSafety Commissioner, *Unwanted contact*. At https://www.esafety.gov.au/esafety-information/esafety-issues/unwanted-contact
6 Office of the eSafety Commissioner, *Offensive or illegal content.* At https://www.esafety.gov.au/esafety-information/esafety-issues/offensive-or-illegal-content
7 Office of the eSafety Commissioner, *Photos, videos and social media*. At https://www.esafety.gov.au/education-resources/iparent/staying-safe/photos-videos-and-social-media
8 Office of the eSafety Commissioner, *Offensive and illegal content complaints*. At https://www.esafety.gov.au/complaints-and-reporting/offensive-and-illegal-content-complaints
9 Office of the eSafety Commissioner, *Legislation*. At https://www.esafety.gov.au/about-the-office/legislation
10 Office of the eSafety Commissioner, *eSafety issues*. At https://www.esafety.gov.au/esafety-information/esafety-issues
11 Office of the eSafety Commissioner, *Protecting personal information*. At https://www.esafety.gov.au/esafety-information/esafety-issues/protecting-personal-information