



Respecting the Online Rights of Children and Young People

Commissioner for
Children & Young People
February 2021



When it comes to dealing with young people's personal information it is important to be mindful that the most valuable commodity in the evolving world is data. More than this, data is inextricably linked to the individual identity of its owner. We therefore have absolute responsibility to ensure that when young people share their data with us, we treat it with the care and respect it warrants.

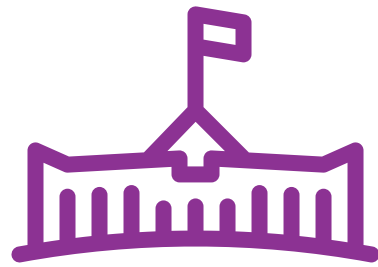
We want children and young people to embrace the internet to learn, share, collaborate and participate in civic life, with free expression. Simultaneously, we need to protect the rights of children and young people to ensure they benefit from all that the internet offers them, without coming to any harm.

While there are many places online, which require us to educate children and young people to be particularly wary, dealings with South Australian agencies, organisations and industry should never be amongst them.

It is imperative that these agencies, organisations and industries consistently adopt best practice policies and procedures that ensure children and young people can visit safe online places they know they can trust and confidently access.

Responsibility for children's online rights

We all have some degree of responsibility when it comes to respecting young people's rights in South Australia:

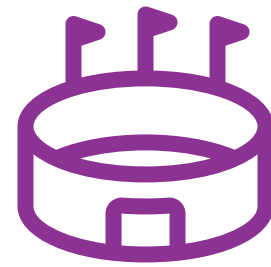


Federal and State governments have primary obligation to protect children's rights to both privacy and freedom of expression while online. Legislation and policy has been designed to enshrine these principles of protection so that they can be uniformly communicated to relevant organisations and bodies whose compliance is monitored against the standards set.



In South Australia, **organisations, agencies and businesses that interact with children and young people**, must develop and implement a Child Safe Environments Policy and associated set of policy and procedures. This includes local councils and private businesses that work directly or indirectly with children and young people.

Adopting child safe principles means asking what is in the best interests of the child and acting to put in policies and procedures in place that support this. It also means ensuring that children and young people can interact safely with staff and resources as well as be given opportunities to provide feedback in a secure, non-threatening manner.



Organisations who invite children and young people to voluntarily interact with them, must ensure that they are kept safe at all times. Upholding a child's right to participate, means putting stringent guidelines in place to ensure their protection while they are doing so; particularly those organisations that conduct research directly with children and young people themselves (see <https://www.childethics.com/>)



Parents need to speak with children about their rights, and explain what they can expect when participating and interacting with organisations, businesses and service providers in the online environment. They should also speak about what not to expect and how to communicate their concerns around 'interactions that don't feel right'.

By encouraging age-appropriate 'street-smart' behaviour, without overemphasising risk, or taking a fear-based approach, children will be able to navigate their online world more confidently.

The challenge for adults is to strike the right balance, using common sense and an even-handed approach; one that shows respect for the rights of child and young person concerned to participate, while simultaneously ensuring they are kept safe and protected while doing so.



Children and young people have a right to know whether someone is holding or making money from collecting their personal information, as well as what their information is or will be used for, including whether it is being copied, sold, or traded to third parties.

Children and young people need to know upfront that they have a right to privacy and that if or when they do not wish to provide personal data there is no requirement to do so. Or when they do decide to provide their personal data, that it is being protected.



To safely interact with children and young people online organisations should look at incorporating the following tips:

Ensure good data collection and storage policies that protect children's privacy are put in place.

Organisations should ensure they have a clear privacy policy that includes how children's data will be used and how it will be protected.

Top tips include:

- Agencies / organisations should make it clear they will not publicly share personal data about children who have engaged with them without genuine informed consent. This means agencies/organisations wishing to use information provided by children need to publish child and youth friendly terms and conditions so that a typical young person is realistically able to read them all and fully understand them. Alternatively, a policy ensuring that when or if information of a personal nature is collected, that it will only be shared with those the young person has genuinely granted consent to do so.
- Industry should not collect or monetise children's data.
- Parents should not intrude on children's privacy without their consent. This includes not using invasive third-party monitoring features currently available on some social media accounts.

Children and young people should be provided with an option that enables them to quickly, and without question, retract any information they decide they do not want to remain in the public realm at any time.

Agencies / organisations should offer simple ways for children and young people to retract, delete, or remove any information they have supplied.

Top tips include:

- Make it clear to children and young people at the start of any online survey, consultation, or other type of engagement, that they can opt-out at any time.
- Provide multiple ways for children and young people to contact an organisation with whom they interact online. This could include building in a mechanism where a child or young person can ask to opt-out without any questions asked, and without any requirement to talk to someone about their decision.
- Parents exercise care and caution when engaging in the practice of 'sharenting'. (Access CCYP's factsheet on Sharenting: <https://www.ccap.com.au/wp-content/uploads/2020/03/202002-Fact-Sheet-Sharenting-V3-1.pdf>)

Being mindful of the long-term repercussions of a child or young person's digital footprint

Agencies and organisations should not store a child or young person's digital footprint in any way that could identify them. This means examining the ways in which information about children and young people is collected and distributed within an organisation or agency. Just as with adults, collecting and storing information obtained via a child's digital usage and interactions, always increases the risk of it being shared. It also heightens potential for third-parties to access and use this personal data in ways that may result in inappropriate contact being made, or inappropriate content being sent to the child or young person whose digital footprint was tracked and stored.

