

insights

Protecting your child's online privacy

by Colin Anson



From sharing pictures of a child's first day at school to key moments at high school, many adults don't consider the potential risks or breach of future privacy for kids. In fact, it is now become a ritual to announce the full name and date of birth of a child online within hours of them being born. This is just the beginning of a child's digital footprint.

Although children are now 'born digital', exposure in the online world can present just as many risks as the physical world can pose. Images and identifying details can be used for numerous activities that put your child at risk, from stalking, to cyberbullying, identity theft, and even digital kidnapping.

The Australian eSafety Commission warns that half of all images on paedophile image-sharing sites originate from social media sites and blogs. Parents are responsible for protecting kids until they are old enough to make their own decisions about their online presence.

So, what can parents do?

Start by 'thinking privacy' before posting images of children online. You'll be protecting their digital footprint and setting them up for a healthy relationship with the digital world.

Seek consent

Always ask others before sharing images of their children, even your family. Speak up about how you feel about images of your child being shared. When your child is old enough, ask them for consent, empowering them to understand they have a right to their privacy online. As they become teenagers, hopefully they will have more respect for what they post online and have confidence to speak to others about their consent guidelines.

Understand the settings

Check the settings of your social media channels to ensure your posts are not public. Speak to your friends and family about this and don't be afraid to ask for help to get it right. If your child has social media channels of their own, go through the settings with them to minimise the risk of unwanted shares.

Think about the detail

Avoid including children's identifiable details such as school badges, logos, uniforms, name tags or identifiable locations such as your home area or school. Alternatively, blur these details prior to posting.

Be selective

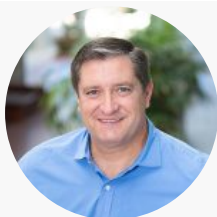
Create a simple checklist to help make decisions regarding posting online easy. What do you deem appropriate? Are you happy to share images of your children in swimwear? Do you want to avoid full-frontal face shots?

If your child is old enough, explain why you are selecting certain pictures and not sharing others. If you have a teenager who is sharing their own images, talk to them about what is appropriate and potential repercussions of not setting boundaries.

Remove metadata

Metadata on digital images records the time, date and GPS coordinates of where the photo was taken and can be accessed through shared images, and your sharing service may record your IP address. You can wipe this information with appropriate software or share screenshots of your photos to avoid metadata sharing. Screenshot sharing creates a lower resolution photo, so it's less likely to be tampered with by a third party.

Think 'privacy first' to reduce many of the risks involved with image sharing. Have conversations with your children to instil this mentality; help them build empathy; and identify the steps for minimising risk whilst helping them build a healthy relationship with technology so they can become responsible digital citizens.



Colin Anson

Colin Anson is a digital entrepreneur, and the CEO and co-founder of child image protection and photo storage solution, pixevety. Find out more about Colin at pixevety.com.