



RESOURCE BOOKLETS for Kinship Carers

**Cyber safety for children
& young people**

Carer Kafé





GPV/KCV acknowledges the peoples of the Kulin nation as the traditional owners of our great land and offers respect to Elders, past and present.

GPV/KCV acknowledges that the Aboriginal culture existed in Australia before European settlement and consisted of many community groups. Further, we acknowledge the Indigenous peoples of this land as the oldest continuing cultures in human history.

GPV/KCV acknowledges that laws and policies of the past have inflicted grief and suffering on our fellow Australians and regrets the removal of Aboriginal and Torres Strait Islander children from their families.

GPV/KCV believes that a society that is inclusive of all is crucial to individual and community wellbeing and will behave with respect towards all irrespective of their race, religion, sexuality, gender or socio-economic background.

GPV/KCV acknowledges 13th of February as National Apology Day, the anniversary of then Prime Minister, Kevin Rudd, delivering the National Apology to Australia's Indigenous Peoples in 2008. GPV/KCV will take steps that promote a happier and healthier future for Indigenous Australians, particularly the children and young people.

Ph: 0499 969 234

Email: admin@kinshipcarersvictoria.org

www.grandparentsvictoria.org.au

www.kinshipcarersvictoria.org

Key words which influence GPV/KCV approaches are: Truthfulness, Confidentiality, Inclusiveness, Integrity, Constancy, Gratitude, Commitment, Compassion.

This podcast was recorded and produced on Djaara Country, the land of the Dja Dja Wurrung people, and we extend our ongoing respect to all Kulin Nation peoples, the traditional custodians of these lands and pay respect to the elders both past and present and to the deep knowledge of the land that is embedded within the indigenous communities.

Kinship Carers Victoria
acknowledges the support of the
Victorian Government.



Contents

Cyber safety statistics	4
About the podcast presenter	5
What are some of the basic strategies adults can employ to help children and young people navigate their digital world safely?	6
How do you know what is the right amount of screen time for children/young people?	6
At what age should children be allowed to start using online devices? When are children/young people ready for their own social media accounts and their own smart phones?	7
How do adults create a safe gaming environment for a child/young person?	7
This is a podcast for parents and carers, some of whom are older and may not be very tech-savvy. What advice can we give such people?	8
What is cyber bullying, what forms can it take, what signs should a carer watch for to see whether a child/young person is being cyber bullied – and what can be done about it?	8
Children and young people may discover pornography online. What role can adults have in these situations? How can adults protect children/young people from encountering these images?	9
What is grooming of children/young people and how does it happen? How do adults help the child/young person with unwanted contact?	9
What do 'sending nudes', 'sexting' and 'image abuse' mean and how is it best to talk to young people about this content?	10
Useful web pages on cyber safety for carers, children and young people	10
How might parents/carers use different software or tools on devices to monitor or limit what young people see and watch?	11
How can adults help children/young people stay in control of their personal information online?	11



Cyber safety statistics to contemplate before reading further

- Globally, 79% of 15 to 24-year-olds were online in 2023.
- Over a third of young people in 30 countries report being cyber bullied.
- 80% of children in 25 countries report feeling in danger of sexual abuse or exploitation online [The UN].

In Australia,

- Six in 10 teenagers have seen harmful content (drug-taking, suicide, self-harm and unhealthy eating, gory images, and violent sexual material) online which most parents are unaware of.
- Teens (12-17) spent an average of 14.4 hours a week online to research topics of interest, watch videos, chat with friends, listen to music, play games online with others [eSafety Commissioner's report in 2020]
- Four in 10 (44% of Australian teens) had at least one negative online experience, this includes 15% who received threats or abuse online.
- The top three negative online experiences are: 1) being contacted by a stranger or someone they do not know, 2) being sent unwanted inappropriate content, such as pornography or violent content, and 3) being deliberately excluded from events/ social groups.
- 53% of young Australians have been cyber bullied.
- Six in 10 young Australians (aged 8–17) played online multiplayer games, and 1 in 2 reported they played games with people they have never met in person. 34% young people surveyed said they had made in-game purchases and 17% had experienced in-game bullying.
- In 2021, the ACCCE Child Protection Triage Unit received more than 33,000 reports of online child sexual exploitation [Australian Centre to Counter Child Exploitation ACCCE report].
- 67% of primary school children and 36% of preschool children own their own screen-based digital device. One in 6 primary school children and 3 in 4 adolescents had their own social media account. Kids in this survey spend an average of 32 hrs per week on screens at home and 43% regularly uses screens at bedtime [Australian Child Health Poll].
- Australian 11–16 year olds had exposure to sexual images online (encountered by 28%); bullying on the internet (13%); receiving sexual messages or 'sexting' (15%); and seeing 'harmful' user-generated content (such as hate messages, self-harm, drug experiences, 'ways to be very thin' and suicide sites) (34%) [2012 report of 400 young Australians and their families].





ADAPTATION of a PODCAST TRANSCRIPT

Cyber safety for children and young people – from a podcast addressed to kinship carers

About the podcast presenter

The podcast that accompanies this transcript was presented by Susan McLean.

Susan McLean was a Victorian police officer for 27 years who took her first report of cyber bullying in February 1994, when she became aware that technology could be misused. Susan trained with the FBI in the US and worked with the Dallas Police Department's Internet Crimes against Children Task Force team.

Upon her return to Australia, she was the first Victorian police officer given a position looking at online safety for young people and she completed university studies in England and America before leaving the police force 15 years ago to start her own consultancy. She educates around 400,000 students and tens of thousands of adults every year right around the world.



Cyber safety for children and young people

What are some of the basic strategies adults can employ to help children and young people navigate their digital world safely?

Susan McLean – *It's really impossible to be 100% safe online because every time technology is used there is a risk. It's important to make sure that parents and carers actually understand what the risk is so they know what is out there, what it looks like, how it might happen and then understand the steps to avoid it or reduce the likelihood of it occurring. First of all, we have to accept that every person, young or old, that uses technology is at risk and that there are different levels of risk.*

Young people are vulnerable to online harm for a variety of reasons – including their mental health, perhaps homelessness, or it may be because there's illness in the family – they are especially vulnerable because they see the Internet as a safe place to be. They will connect with people whom perhaps they might not normally, which can sometimes lead to potential harm. Parents and carers should be involved in their child's online world – supervising time spent online, understanding the platforms their child is using and when to say 'no'. Parental controls both on devices and online platforms are a good tool to use, but it is just as important to ensure conditions of use for particular platforms are followed, including age restrictions of users. It's important that parents and carers aren't enabling misuse of online services by lying about children's ages, potentially putting them in harm's way.

How do you know what is the right amount of screen time for children/young people?

SM – *There are two parts to screen time: the amount of time and the content.*

Firstly, the time must be manageable – if the amount of time a child is spending on screens is interrupting the smooth running of a household, then that is probably an indicator that there is a problem. This could include refusing to participate in meal times or staying up past bedtime. In general, less is better – children should be outside, engaging in play and exercise. Too much screen time can negatively impact this.

The next step is to look at what they are doing online, and making sure that we're aware of the content that they are consuming. Online tools can be great learning resources and beneficial for some aspects of schooling, whereas R-rated sites should be inaccessible for young people.

One of the key messages from the American Society of Pediatrics is no screens for under twos, which is considered to be best practice globally. That doesn't mean no Face-Timing grandparents, for example, it means don't give an 18-month-old an iPad and come back in three hours. We really need to have zero or minimal screen time for under twos because the brain is in a vital developmental stage at that age.

Cyber safety for children and young people

At what age should children be allowed to start using online devices? When are children/young people ready for their own social media accounts and their own smart phones?

SM – *Providing a child with a smartphone does not keep them safe; it does the opposite. While parents often think that giving their child a phone so they can call in case of an emergency is a way to keep them safe, instead this often sets them up to be robbed, cyber bullied or groomed online. There are a lot of risks in giving a smartphone to a child. Providing a child with a 'dumb phone' that allows them to receive and make phone calls but has no access to the Internet or a camera can be an alternative.*

In my experience, there is not a nine-year-old in the entire universe that needs a mobile phone. They might want one, but they don't need one. As a rule of thumb, most parents will give a child a phone to start high school, at a time where independence develops.

In relation to when children should start using social media, every single social media platform has a legal minimum age of 13, so there should be no conversation before 13. Parents can communicate with their children without using a social media platform.

There's nothing wrong with the occasional use of a device for a younger child, and in terms of educational uses, different schools implement technology at different stages.

A child is not going to be disadvantaged if they don't use an iPad until grade 5. Instead, they will be less likely to experience eye strain issues, musculoskeletal issues and carpal tunnels. As well as the endless physical benefits of not having children sit on a computer screen all day.

How do adults create a safe gaming environment for a child/young person?

SM – *Gaming requires a few considerations: firstly, parents/carers need to download and play the game, allowing them to decide if the game's content is suitable for the child. After content, the biggest risk factor in games is the chat function. Enabling safety features and controlling voice and text chat can make the game safer. If the game is suitable and the chat is off, the last thing to manage is usage.*

It has been found that children as young as eight are being found by paedophiles on games like Roblox and Fortnite. Roblox has a lot of really inappropriate sexual content on it – just because the game is pitched at children does not make it safe. Anywhere a young child is, paedophiles will follow.

“ ... just because the game is pitched at children does not make it safe. Anywhere a young child is, paedophiles will follow.”

Cyber safety for children and young people

This is a podcast for parents and carers, some of whom are older and may not be very tech-savvy. What advice can we give such people?

SM – If parents/carers are not confident with their technology use, I would highly encourage them to learn because technology is a part of life now, especially for young people. A lot of community centres, councils, university of the third age, and even schools offer lessons regarding technology use.

Another recommendation would be to connect with the IT department at the child's school and ask for some assistance. They are very receptive to these sorts of questions and concerns and often more than willing to help.

What is cyber bullying, what forms can it take, what signs should a carer watch for to see whether a child/young person is being cyber bullied – and what can be done about it?

SM – Cyber bullying is bullying online; it can happen on any app, game, site or platform that allows communication. Bullying is repeated – it happens more than once. The most common form of cyber bullying is a nasty message or post, but it can also be intentional exclusion online. It can be setting up of fake accounts, sharing of sexual imagery, posting threats, racist or homophobic comments. All of these things can form cyber bullying, and cyber bullying is a criminal offence in every state and territory in Australia, which means it is a crime and it means that a person engaging in cyber bullying can be arrested. At its most serious, cyber bullying is a jailable offence.

If a parent becomes aware that their child might be getting cyber bullied, they must be aware there are not always obvious signs and symptoms. This makes it important to investigate subtle changes to their child's demeanour or behaviours. The child might have had a falling out with a friend at school, they might have been yelled at by the teacher, they might have failed a maths test – or they might be having a problem online.

It can manifest itself with what I call 'phantom ailments'. That is, complaints of issues that don't have a true medical cause; for instance, stomach aches or headaches that spontaneously resolve five minutes later. The sorts of things that suggest something is not right may have a different root cause.

If a child is cyber bullied and a carer becomes aware of it, it's important to praise the child for speaking up because voicing it is essential and is very hard for children to do. It's necessary to then document and make copies of the evidence, as that will become needed when reporting the abuse. First, report the abuse to the platform and then block the user – it must be done in that order, because blocking first stops the ability to report.

The next step would be to inform the school; this could be a teacher, year level coordinator, or wellbeing officer. Over 90% of all cyber bullying at school is resolved adequately if those steps are followed.

Cyber bullying is a criminal offence and if it's a fake account or if threats have been made to the child's personal safety, it needs to go to the police so they can identify the person behind the account. Another resource is office of the E-Safety Commissioner. Their website esafety.gov.au has some basic factual information relevant to parents.



Children and young people may discover pornography online. What role can adults have in these situations? How can adults protect children/young people from encountering these images?

SM – Australian statistics show that 80% of 12-year-old boys, 100% of 15-year-old boys and 80% of 15-year-old girls have seen pornography. The chances that children are going to come across it are high.

The main problem with pornography is most of the content viewed currently includes violence – it's not what some carer's perception of Playboy or Penthouse magazine might have been. Contemporary online pornography is quite violent, shows unrealistic body types and sexual acts. A lot of young people are using pornography as a sex education tool and they're assuming that what they're watching is real, then trying it and sustaining quite serious injuries. We see girls that have been choked. Often we see girls that have been internally torn. I've even had a 15-year-old boy that snapped the shaft of his penis when he was engaging in what he described to his father as 'rough sex'.

At home parents should make sure the Internet is filtered, making pornography sites less likely to be found. Parents should put in place all available control measures, but understand that they can't control another child at school showing it to their child.

There is a really useful website called itstimewetalked.com run by Marie Crabb who is a real expert in the effects of pornography on young people. The current campaign that she's running is called 'Porn is not the norm', and she's done extensive research in relation to the effects of pornography on children on the spectrum. The website contains relevant information for parents for both neurotypical and neurodivergent children.

What is grooming of children/young people and how does it happen? How do adults help the child/young person with unwanted contact?

SM – The issue of online sexual abuse of children and grooming is hideous and it's growing at an extensively high rate because it is the fastest growing crime type in the world.

Ninety-nine percent of young people will not engage with a random stranger in real life. They will not go to the shops and just talk to people; they will not talk to random people on the street. But on the Internet they do. Over 90% of all online child sex offenders are not known to their victim in real life. Parents/carers should regularly check children's contact lists, game lists and chat lists to make sure they are not talking to people they don't know.

Is this going keep children 100% safe? No, because nothing is, but they're going to be far safer than if they are able to engage with random people. Children will use the term, 'it's my online friend.' An online friend is a term that children use to describe a random stranger who is being nice to them.

Cyber safety for children and young people

What do ‘sending nudes’, ‘sexting’ and ‘image abuse’ mean and how is it best to talk to young people about this content?

‘The Australian Federal Police ... were seeing children as young as five years of age taking photos of themselves naked and posting them on the Internet.’

SM – The issue of sending nude images is not new. It’s been around for as long as mobile phones have had cameras. In the early days it was really only adults sending nude images because they were the only ones who could afford the phones. But now if a child has access to this technology, then they have an ability to participate. Last year the Australian Federal Police put out a media release saying that they were seeing children as young as five years of age taking photos of themselves naked and posting them on the Internet. We know that many teenagers use sending nude photos as part of their flirting and dating process.

The compounding issue for young people is that a naked or sexually explicit image or video of a person under the age of 18 years is classed as child abuse material and that means they can be arrested and charged. There are young people who intentionally commit criminal offences, but there is a vast majority of young people who may choose to send nude photos without criminal intent, yet they get caught up with these laws.

These laws were written to protect children from paedophiles, so they’re robust, legally sound, and there’s no discretion and no loopholes, which is exactly what we want when we’re dealing with paedophiles. But if we’re dealing with a child that really has made an honest mistake, we need to do better. Victoria is the only state in Australia that has slight amendments to these laws, and what we have in Victoria is basically four boxes that the police can tick. If they tick those four boxes, then the young person will not be charged with one of these crimes. The four boxes are: there was no threat for their coercion, threats to further share the image or further sharing; there is no more than two years age difference between the people sharing it; there is no adult involved; and no other criminal act is depicted in the photo. Provided those four things can be ticked off, the police will talk to the young people about choices and the fact that this is going to end in tears but no criminal charges are laid. If, six months later, one of the parties decides to share the image, charges can be laid at that time.

USEFUL WEB PAGES ON CYBER SAFETY FOR CARERS, CHILDREN AND YOUNG PEOPLE

<https://www.esafety.gov.au/parents/issues-and-advice/parental-controls>

<https://www.childsafe.org.au/help-for-families/e-safety-online/>

<https://www.vic.gov.au/parents-and-cybersafety>



Cyber safety for children and young people

How might parents/carers use different software or tools on devices to monitor or limit what young people see and watch?

SM – Enabling parental controls on your modem will help limit what children can access. On top of that, a filtering product adds extra protection as well as virus protection on individual devices.

Another strategy to implement is a ‘family safety contract’, or a written document between the adult and the child outlining the expectations for tech use in the house. This is establishing a base level understanding and agreement that can be referred back to.

Further, every single digital device in the house, whether that’s a gaming console, a smart TV, iPad, iPod, mobile phone, laptop or desktop will have parental controls in it. It is a matter of enabling the parental controls in the device. For most families, that is going to be sufficient. If these three things are implemented together, families will have pretty good success.

Third-party products are additional layers of protection that can be beneficial for families with a child diagnosed with a mental health concern; for example, perhaps they have anorexia, where an extra level of protection is necessary.

How can adults help children/young people stay in control of their personal information online?

SM – Cyberspace is a public place, not a private space. When speaking about the Internet, safety is the only thing that can be achieved, not privacy. Everything posted on the Internet is no longer owned by the original poster, so thinking before posting is crucial. Certain strategies can increase privacy measures, such as locking social media accounts and making them private, ensuring friends lists are not public, and using non-identifying profile pictures. Other precautions can include turning off location services on the phone’s camera, managing tagged photos and mentions on social media. The Internet provides access to a different world – the more effort put in to ensuring that world is as safe as possible for the user, the better the outcome.

This podcast was made possible by generous support from the Department of Families, Finance and Housing and Carer KaFE.

To listen to or download any of KCV's podcast series, click here:

<https://kinshipcarersvictoria.org/podcasts-videos/>



Kinship Carers Victoria
0499 969 234
admin@kinshipcarersvictoria.org



Families,
Fairness
and Housing

Kinship Carers Victoria
is supported by the Victorian Government.

Carer Kafe'