Talking to children about digital privacy

At every stage in your child's development, there is an appropriate way to talk about their privacy and the value of their information. Even from a very young age, conversations and activities can be introduced to establish a framework for building knowledge, independence and confidence. Below are details about how you can talk to children at different ages.

CHILDREN AGED 3-5

Australian children in this age group are likely to have access to a device which belongs to their parent or caregiver and will use it mostly for playing games, watching media and connecting with relatives (e.g., on skype or zoom). They will have some idea about some potential dangers from the Internet, such as accidentally finding inappropriate or scary content, but they won't see sharing personal information as something to be worried about.

Parental protection is very important as children 3-5 do not recognise risks to their privacy and will freely share information when it is requested. At about the age of 4, children will start to grasp the idea of secrecy, which is an important step in learning to manage their privacy. Supervision, particularly over which apps are downloaded and whether they have adequate privacy controls is needed.

This is the perfect age to introduce basic concepts and terminology about the Internet and about privacy. It will provide a good foundation for digital literacy and cyber-safety education, making it easier for children to learn more advanced concepts when they are older.

Here are some concepts you can introduce to your 3–5-year-old child:

What is the Internet?

Explaining what the Internet is to small children is very difficult and you do not need to get too technical. This is about starting a conversation and helping children to understand something complex.

To keep things really simple, break it down into the two concepts of 'connection' and 'sharing', because this is really what it's all about.

Keep your explanations simple, and if words aren't your thing, doing simple drawings with your 3–5-year-old is a fantastic way to get them thinking about it.

A good way to describe a complex concept to a very small child is to relate it to a concrete example that is familiar to them and easy to visualise. Here is an example of how you could talk about *The Internet*. Remember that using drawings and hand movements will really help get these ideas across.

> ***The Internet is like a tree.***
>
> *On a big tree there are many, many branches and thousands of little leaves. Each little leaf is connected to every other little leaf, even if they are on different branches.*
>
> *If one little leaf wanted to send a message to another little leaf on the other side of the tree, they could send their message down the branch, around the trunk, up the other side and all the way to their friend on the other side.*
>
> *This is how we use the Internet! Our computers (phones, tablets, etc) are just like the little leaves, connected to other computers around the world. Because computers are connected to the Internet (which is a bit like the big strong trunk of a tree), we can share all sorts of information with other people. We can share messages and music, photos and videos, talk to our friends and play games.*

Asking questions is also a great way to get your child thinking about what the Internet is. Here are some examples:

> *What kind of devices do we have in our house that use the Internet?*

What is your favourite thing to do using the Internet?

What activities are 'online' and what activities are 'offline'?

Learning to recognise when we are 'online' and when we are 'offline' is really important. It might seem obvious to us as adults but for very young children, connectivity is so integrated into the way we live that it is not always clear. This is an important concept because it helps young children to understand and differentiate when it is appropriate and safe to share information and when it is not.

Fortunately, this is not a difficult concept to grasp, and with repetition and consistency children will pick it up very quickly.

A simple way to talk about this with your children is to ask them whether activities they enjoy are 'online and sharing' activities or 'offline and private' activities. You can start with the most obvious activities and as your child gets older you could challenge them to work it out for activities that are a bit more ambiguous. Here are some examples:

When you are reading a book with Daddy, are you online and sharing, or are you offline and private?

When we are talking to Nanna on the computer, are we online and sharing, or are we offline and private?

When we play on the beach, are we online and sharing, or are we offline and private?

When you are watching YouTube Kids videos about funny cats, are you online and sharing, or are you offline and private?

What is 'My Information'?

Learning to value our personal information starts with recognising what it is and having the language to describe it.

Children aged 3-5 already know a lot of personal information about themselves. They know that it's part of their identity, and that they can 'give' that information to people who ask for it (*What's your name? How old are you?*).

At this age, simply introducing the idea of 'my information' and asking children to work out what kind of information 'belongs' to them is enough. It can instil a sense of ownership and autonomy over their personal information.

Here is an example of a very simple activity you could do with a 3–5-year-old child:

This is a two-minute activity that combines action, words and touch – making it easier for children to remember. We have used toes and feet because later on, when they are learning what a 'digital footprint' is, this visualisation could be useful.

*Ask your child to wriggle their toes. Maybe they can stretch their leg out and try and reach their toes or maybe they need to cross their legs to reach their toes. Wriggle your own toes and then point and touch each toe individually, saying this phrase (one word for each toe) "**My - Information - Belongs – To - Me!".** Then go back and for each toe think of some personal information that belongs to you, like your name, your age, your address, your phone number. Ask your child to copy you, first saying the phrase as they touch each of their toes and then trying to think of five different types of personal information.*

This could be turned into a game if other family members join in or could simply be a starting point for your child to ask you questions about personal information.

CHILDREN AGED 6-8

Australian children in this age group are very likely to have a device of their own, or access to family devices, and will be using it to play games, media and also for educational purposes. At this point, not many children have their own mobile phone. They may be starting to learn about cyber-safety at school and are getting better at identifying inappropriate content or online situations that are unsafe. They may be less adept at knowing how to respond appropriately to these.

Whilst they are developing a sense of privacy within their social networks, and they care deeply about how their personal information is shared between their peers and their family members, it is difficult for them to understand that personal information is being collected by people or organisations that they don't know. Such children are not yet aware of tracking and do not have the skills to manage their privacy online. It is crucial that parents offer hands-on guidance, clear rules, and effective supervision to protect their children's privacy online.

Children aged 6-8 are still looking to their parents for cues on the right ways to act and behave so this is the perfect time to model good privacy management and show your children *how* you do that. This will help them to learn the necessary skills for identifying traps with apps and steps they can take to protect their privacy.

Here are examples of activities, discussions and strategies you can use with your 6–8-year-old:

Ask first and Learn

Ask your child to come and let you know each time they want to download a new app on to their device (or the family device). Take enough time to look at the app with them and decide whether it is safe for them to download. Share how you make that decision with them and tell them why you think an app is safe to download or why you think it might be unsuitable. For example:

> *Hey, I think that game looks like it might have some really nasty violence in it. I'm not happy letting you download that one. Why don't you find another?*

Or

> *That app looks like a lot of fun and I can't see anything that makes me feel worried. Let's download it and see what kind of information they want from you.*

Go through a basic privacy check on the app, looking at the requests that it makes and deciding whether it is reasonable. Turn off many of the permissions that are not really needed. Once again, talk it through with your child and encourage them to be part of the decision making. For example:

> *Let's just see what kind of things this app would like to be able to do…..oh they would like to see the photos we have taken – do you think they need them for this game? I think we could turn that off so they can't see our photos. Let me show you how we can do that.*
>
> *This app would like to know our location, even when we are not playing the game, what do you think about that?*

The Weekly or Monthly 'check-up'

As well as the activity described above, regular 'check-ups' can be done. Or, if you are time poor, is still helpful to make the time to focus on this one.

Weekly or monthly, plan 15-30 minutes to sit down with your child and the device that they use. You could do this either one-to-one or even as a family all together around the table. Together with your child, do a privacy check on each app that they have on their device. Delete apps that they no longer use and check to see that no new apps have appeared without you knowing. Also revisit the privacy settings on the device to make sure nothing has changed.

As suggested above, talk through each decision and process with your child and involve them by asking what they think. This process will help them become familiar with basic terminology that is used in privacy policies and give them a framework for managing personal information.

Building literacy

Revisit and re-learn the concepts that you taught your 3–5-year-old: *What is the Internet? When am I online and when am I offline? What is My Information?*

Here are some examples of new concepts that 6-8 year-olds are ready to take on:

My Digital Footprint

Your digital footprint is all the little pieces of information that you leave about yourself when you use the Internet. It can be made up of visible things like photos or messages that you share with friends. It can be information about you, like your name and your age, but it can also be invisible things like what videos you enjoy watching or how you play Minecraft.

Tracking

Tracking is how companies collect information about what you do when you are online. Tracking is done with little pieces of information (snippets of code, sometimes called 'cookies' or 'trackers') that live on your device or your computer and they tell companies about the kinds of things you look at or do on the Internet. These little snippets of code are put on your device when you download an app or even open a website.

CHILDREN AGED 9-12

In the upper primary years, many Australian children will be transitioning from using the family device to having their own personal device, and even to owning their first mobile phone. They are beginning to explore the online environment and use it to develop a sense of identity. 9–12-year-old children are good at questioning the world around them and are starting to develop critical thinking skills. They are very aware of social pressure and are starting to shape themselves to 'fit in' with their peers.

At this age, many children will have a good understanding of inappropriate content, understand that they shouldn't overshare information, and will be cautious about strangers that they meet online. However, parents should definitely take it with a pinch of salt when their 9–12-year-old child reassures them that they '*know all about it from school*' – because it's still difficult for them to apply their knowledge to real-world situations, no matter how confident they feel. From ten, children are starting to understand that sharing information online could be risky, but there is still little awareness about third party tracking and the collection of their information.

About this time, children start to look to their friends for guidance and this influences their decision making. They may also want to test the rules and feel reactive and rebellious (*I'm not a child anymore!)* – sometimes choosing to ignore the guidance of their parents. For this reason, these children are particularly vulnerable to oversharing, rule breaking, and risky encounters on social media. They should not have access to risky platforms without adequate supervision and parent engagement.

Here are some ideas and strategies for your 9-12-year-old child:

The Weekly or Monthly 'check-up' – taking it on independently

If you have already been implementing this strategy in your family regularly then this will be a fairly easy step to take. If you are just jumping in, then it's a good idea to start by reading the section above for 6-8-year-olds.

Continue to do either one-to-one or whole family together meetings where you spend 15-30 minutes having a look at the apps on your devices, checking what requests for information they make and revisiting the privacy settings. Delete old apps that are no longer being used.

At this age, encourage your child to do the check-up independently but with your supervision. Ask them why they make decisions about what they allow apps access to on their devices. If you don't agree, explain why rather than just taking over.

If your child is starting to use messaging services (like *WhatsApp* or *Facebook Messenger*), email or even social media, incorporate conversations about these platforms into your regular check-

up. Ask them questions about who they communicate with, what kind of information they are sharing, and whether they are feeling safe.

Making a safe space

This is the time to prepare children for the greater independence of adolescence. When children become teenagers, they are going to have access to a whole range of content and platforms that have so-far been off limits (having their own social media accounts etc.). There will be more requests for information than ever before and more sharing information online with their peers. This is both exciting and overwhelming.

Rather than just having them jump in at the deep end the moment they turn 13, or start high school, use the years between 9-12 to talk about the responsibilities of having a social media account. Let them see your account if you have one (or perhaps a relative's if not) and show how you use it. Spend time on it with them answering any questions that come up and demonstrating how to adjust privacy settings. This is a good age to establish that they can talk to you about issues that they encounter when they are online – things that feel uncomfortable, threatening or confusing. Make it clear that such talk will be non-judgemental and compassionate. Here are some examples of what we can talk about to children at this age:

Oversharing

What we put on the Internet is never private, and it never disappears. So think really carefully before sharing messages and photos. Would you mind if your mum, your teacher or your doctor saw what you were thinking of posting on social media? Even if you think things are private, they are still being stored on the Internet. Be yourself but be safe! It is very easy to lose control of the information you share on the Internet.

Who can we talk to?

Ask your child to identify at least two or three adults who they know and trust that they can go to for advice, help or support if they are feeling out of their depth online. For example, if they share information that they wished they hadn't, or if they have met someone online who is asking them for information that they are not comfortable about giving, or if they are being bullied. Create some safe and non-judgemental spaces for them.

Privacy Basics

A simple privacy guide for children to follow when they are online:

- *Don't give out any personal details to people online.*
- *Don't click on pop-ups or ads – they can take you to websites which have either inappropriate content or sites asking for financial information.*
- *Don't put your personal details alongside your photographs online.*
- *If something comes up that makes you curious or uncomfortable or scared – take a screenshot! You can then show a trusted adult and ask their advice.*

TEENS AGED 13-15

At this age, most teens will have sole use of at least one personal device and are likely to be using laptops or tablets at school for education. They will probably use social media, video and gaming platforms for entertainment and connecting to their friends. Social media and peers have become the key source of news and facts. They may use illegal download sites to access free media and entertainment, posing a risk to their privacy.

Young teens are experiencing significant neurological development, and this is changing the way they make decisions and how they evaluate and respond to risk. Some teens will develop a more risk-averse temperament, whilst others will become high risk-takers.

This is a critical moment for the development of mental health conditions, and a key stage to be aware of issues such as low self-esteem, compulsive behaviours and digital addiction.

At age 13-15, teens will really be pushing boundaries and testing out the limits of their parent's digital restrictions. It is hard for parents to get the balance right between being highly restrictive/protective or trying to take a laid-back approach. This inconsistency can create tension and confusion. It can be a good idea to re-evaluate and renegotiate collaboratively with your teenage children to develop an agreed set of boundaries and expectations about their digital habits (time spent, content and platforms they access, information they give out, level of parental supervision etc.) Parents should be aware that although teens would like us to think they know how to manage their privacy effectively, it's more likely that they don't.

At this point, you can start to have interesting conversations with your teens and challenge them to think critically about their online experiences. Keep your language warm, supportive, open and curious to help keep teens engaged in discussion with you and more likely to take on board your concerns rather than 'switching off'. Try not to be too critical and acknowledge the difference between generations.

At this age you need to be talking to your teen about how to safeguard their privacy independently. If this is something you have been discussing and doing together since they were young, then they will know what this means and what is expected of them. Make a monthly date with your teen where you get the chance to have a chat about their digital life, ask them if they've had any issues and make sure you touch base about their privacy settings.

Here are some important topics to discuss with your 13-15-year-old teen:

Digital Addiction

This is the most vulnerable age for developing screen addiction, which can have a really negative impact on a teen's mental and physical health, their relationships and their academic achievement. Talk to your teens about how spending a lot of time on one platform can be really unhealthy for them, a bit like eating too much junk food and not enough healthy food. It is bad for their privacy because companies can collect *a lot* of information about their behaviour. It is also bad for their state of mind. Talk to your teens about what they should do and who they can go to if they are struggling to put their device down and can't seem to get off a specific platform, like a game or social media. Explain to them that those platforms are purposely designed to be as 'sticky', or absorbing, as possible because prolonged engagement with a platform leads to more money for the distributor, so we need to be cautious not to get too hooked in. You can suggest that they should not let others control how they think, feel and behave, especially people who they do not know personally.

You can let your teens know that protecting them from digital addiction is important to you, and if you feel or notice that they are struggling to manage independently, you will intervene and implement some time where they have less access. You can respect their need for independence and autonomy, but this needs to be balanced with their safety.

Revisit Privacy Basics

When your teen is using social media or gaming platforms regularly, here are some basic privacy guidelines for them to follow:

- *Don't give out any personal details to people online.*
- *Don't click on pop-ups or ads – they can take you to websites which have either inappropriate content or sites asking for financial information.*
- *Don't put your personal details alongside your photographs online.*
- *Tell your teens to take a screenshot if something comes up that makes them uncomfortable – they can talk about it with a trusted adult.*

TEENS AGED 16-18

At this age, the majority of teens have their own mobile phone and are also likely to have a laptop for school. Most parents trust their older teenager to manage their own privacy and they spend a lot more time unsupervised and with less restriction than in earlier years. At this age teens are mostly influenced by their peers, but family values are still important to them and still shape their behaviour, so continuing to model healthy digital habits and having clear (but less restrictive) boundaries and expectations remains important.

Although teens are harder to engage than younger children, they also have a lot more cognitive ability and you can discuss things in greater depth and with more understanding. It's important to remember though not to lecture them or dismiss their thoughts. A good approach is to depersonalise issues by discussing them *in general terms* rather than specifically about your teenager. They appreciate concrete solutions to issues rather than just vague warnings about risks and dangers. Just as for younger teenagers, keeping your tone warm, positive and curious will go a long way.

One of the biggest challenges to privacy in this age group is a sense of apathy, complacency and helplessness about companies collecting data. Teens often feel that sharing data with advertisers is an acceptable trade-off and find it very hard to recognise that there could be negative consequences either in the present or future. This lack of motivation is a big barrier to independently managing privacy.

Here are some important topics to discuss with older teens:

Targeted Advertising

Many teens in this age group will have access to personal spending money, and this means that online purchasing increases. With this comes increased vulnerability to the persuasive effects of targeted advertising and also to identity theft and fraud. We can decrease the risk by talking about:

- The link between personal information and the advertising that we see online. Developing a healthy scepticism and critical thinking about persuasive marketing techniques.
- Learning how to evaluate when and where it is safe to provide payment information.
- What to do if you think that your payment details might have been compromised. How do you access help?
- *Nobody is immune!* Teens tend to have the attitude that identity theft and fraud only happens to others, but not to them. Try to break down this barrier and be clear that it can happen to anyone at any time. The only way to protect yourself is to manage privacy carefully.

Managing your digital footprint

Teens do not have a fully developed sense of the longer-term consequences of their actions. We can increase their understanding by talking about:

- Access of their digital profile by future educational institutions or future employers. What are the implications of this?
- Who is allowed access to our information, including our online activity like browsing history or purchase history? As an example, do they know that their web browsing history is not private and can be accessed by charities and councils through their IP address?
- What are the best ways to manage our digital footprint? Ask your teens to show you the strategies they use. For example, are they learning to delete and archive their information on platforms they no longer use?

Persuasive Design and Digital Addiction

Teens may not know that their activity on many platforms (particularly gaming, social media, video and shopping platforms) is tracking their activity and behaviour and using that information

to keep them hooked in. The more they use a platform, the more data can be mined and the more advertising they can be exposed to. These platforms are tailor-designed to be as 'sticky' and absorbing as possible so that the user stays on the platform longer and is more likely to keep returning to the platform. We can help raise awareness and reduce the chance of digital addiction by talking about:

- What do they know about how companies use their data to keep them playing and using for as long as possible? Do they understand the concept of persuasive design?
- When do we know that we are spending too much time on digital platforms? Is it a problem when it starts to interfere with your education, your relationships or your physical and mental health?
- Who can we speak to if we are feeling 'addicted' to our online devices?

NOW IS THE TIME TO TALK TO YOUR CHILDREN ABOUT DIGITAL PRIVACY

Your children's privacy is worth protecting. Even from a very young age conversations and activities can be introduced to establish a framework for building knowledge, independence and confidence about digital privacy. These conversations can range from introducing 3-5 year-olds to basic concepts and terminology about the Internet and about privacy, using practical examples like their foot and toes to convey the idea of a digital footprint, to conversations with teens about persuasive design and digital addiction. Safeguarding your children's privacy until they are old enough to take it on independently involves creating a safe space for conversation, building digital literacy, regular 'check-ups' and privacy basics. Using these simple strategies, and doing it together, parents can reduce the risks and help their children to learn.

For detail about what information apps collect and the risks for children's digital privacy, read our guide, *Children's digital privacy – what are the risks?*

For some practical tips and advice, read our guide, *Steps parents can take to protect their children's digital privacy*.

https://childrenandmedia.org.au/app-reviews/apps-can-trap-tracking

****

MACQUARIE University

Produced in partnership with the Macquarie University Department of Psychology.

accan

ACCM acknowledges the support of the Australian Communications Consumer Action Network (ACCAN) which funded the research for, and publication of, this document.