Talking to children about digital privacy (summary)

At every stage in your child's development, there is an appropriate way to talk about their privacy and the value of their information. The following highlights ways to talk to your 3-5, 6-8, 9-12, 13-15 and 16-18 year old.

CHILDREN AGED 3-5

At this age, Children know that the Internet has potential dangers, but do not recognise privacy risks. Parental protection and supervision are very important. This is the best age to introduce basic concepts and terminology about the Internet and about privacy, making it easier to learn more advanced concepts later.

What is the Internet?

Explaining what the Internet is to small children is very difficult and you do not need to get too technical. 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 an abstract concept to a very small child is to relate it to a real-world example that is familiar to them and easy to visualise - for example a tree, or a road or rail system.

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. 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.

What is 'My Information'?

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, value and autonomy over their personal information.

CHILDREN AGED 6-8

Children in this age may be starting to learn about cyber-safety at school and are getting better at identifying inappropriate content or online situations that are unsafe. However, they do not have the skills to manage their privacy online. At this age, it is crucial that parents offer hands-on guidance, clear rules, and effective supervision to protect their children's privacy online.

Ask first and Learn

Each time your child wants to download a new app onto their device, ask them to come and let you know. Look at the app with them and decide whether it is safe for them to download. Go through a basic privacy check on the app, looking at the requests that it makes and deciding whether it is reasonable. Turn off permissions if they are not really needed. Talk it through with your child and encourage them to participate in the decision making.

The Weekly or monthly 'check-up'

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 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. Talk through each decision and process with your child and involve them in it 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.

CHILDREN AGED 9-12

At this age, 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 starting to look to their friends for guidance and may also be testing rules and feeling reactive and rebellious (I'm not a child anymore!). For this reason, children in this age group are particularly vulnerable to oversharing, rule breaking, and risky encounters on social media. They should not have access to these platforms without adequate supervision and parental engagement.

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

Continue to do either one-to-one or whole family 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. 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.

The Privacy Basics.

- 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

Teens 13-15 would like us to think they know how to manage their privacy effectively, however it is likely that they don't. At this age you need to be talking to your teen about how to safeguard their privacy independently. This is a critical age for the development of mental health conditions and issues such as low self-esteem, compulsive behaviours and digital addiction. Keeping your language warm, supportive, open and curious will help to keep teens engaged in discussion with you and more likely to take on board your concerns rather than 'switching off'.

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. 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 hold their attention and be as 'sticky' as possible, so we need to be cautious not to get too hooked in. Let your teens know that protecting them from digital addiction is important to you, and if you 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.

TEENS AGED 16-18

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. Despite their growing independence, older teens are likely to need some guidance in the following areas:

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 their information, including their online activity like browsing history or purchase history?
- What are the best ways to manage their 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?

****

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.