Optus Digital Thumbprint

Safe and successful

Digital tips for setting up a new device

yes OPTUS

Setting up a new device can be an exciting experience for any young person. A mix of anticipation and curiosity as they explore new features and possibilities. Discussing and agreeing some boundaries around safe use can be a great place to start. This includes a healthy balance of screentime, digital defence moves to help prevent cybercrime, and also tools to help optimise study time.

This guide will help you talk to your child about:

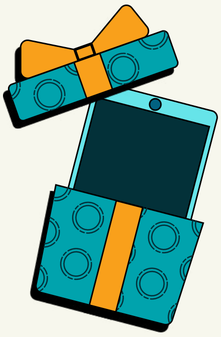
- ✓ Setting up a new device, including enabling the device's safety features
- ✓ What is personal information and how to be cautious online
- ✓ Identifying and protecting themselves from scams and online threats
- ✓ Leveraging tech to enhance their learning
- ✓ Finding help when they need it

Did you know...

82% of Australian parents are aware of online safety tools designed to help young people stay safer online...

...while three in five (57%) still aren't using them on apps and online platforms[1]

[1] Lonergan Research. (2025, June 27). Snap/Ogilvy explores online parental safety controls with Lonergan. Lonergan Research.

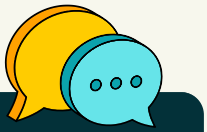


Your child has received their own laptop or tablet.

Start by setting up security tools and parental controls to help them be safe while using the device.

Before you start, explore the device's operating system and familiarise yourself with how to enable parental controls. Parental controls are software tools that when enabled can help keep young people safer online by preventing access to harmful content, managing time spent online and limiting who they communicate with. They are best used alongside additional parenting and online safety strategies[2], and open communication is key when guiding your child's personal device use.

By involving your child in the decision making and reassuring that you are there to help, it will encourage your child to come to you when things go wrong.



Conversation starter:

Your own device is exciting but also comes with responsibility. Can you think of some ways we can keep you and your device safe?

A personal device gives you access to information from all over the world, but it also gives the world access to you! By enabling parental controls on your device, it means that I can help protect you from some of those people who may try to harm you.

Together with your child, agree on a list of rules of use with a personal device. Remember that every family is different and you can adapt depending on the age and maturity of your child.

A sample agreement is provided on the next page.

Get to know parent controls on...

Wi-fi

Some wi-fi routers have software that allows you to enable parental controls that enforces rules on any device connected to that signal.

Operating system software

Major tech software and gaming console companies have many features that can help you keep you and your child safe online. These can include blocking content, restricting sensitive images, limiting screen time and disabling transactions.

Search engines

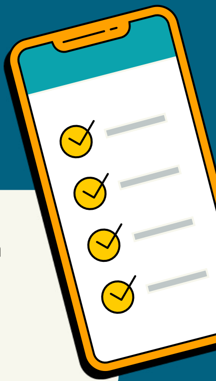
Select a default search engine and enable safe search settings. Consider blocking access to other search engines as a child may use this as an alternative to access certain content.

Streaming services

Streaming services provide built in controls that will filter for age-appropriate content. Set up an individual account for each child and the service adapts content available to their age.

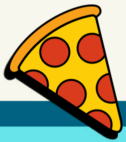
[2] eSafety Commissioner. (n.d.). (retrieved December 1, 2025). Parental controls: How to keep your child safe.

Device Owner Agreement*



Electronic devices can be seriously damaged from exposure to liquid, extreme temperature or falls

- □ I won't eat or drink near the device
- □ I will keep my device clean from spills that might damage its hardware



Software – the programs that run a device – can be damaged by harmful programs created to cause problems

- □ I won't click on strange links
- □ I won't download apps and games without discussing first
- □ I will ask for help to regularly run software updates, including operating system, security software and app updates

Personal information should be kept private when connecting or gaming with people online

- □ I won't share my password or passphrase with others
- □ I won't add or talk to people I haven't met in real life
- □ I won't tell people I don't know where I live or go to school
- □ I will set my account to private
- □ I will keep my full name, date of birth, home address, phone number, email address to myself

Balance screentime with activities and tasks away from your device

- □ I won't spend more than 2 hours of passive screentime per day – like scrolling or gaming
- □ I won't use my device in bed
- □ I will take regular breaks when using my device
- □ I will put my devices away 30 – 60 minutes before bedtime

Cybercriminals target young people for scams and bullying too

- □ I won't interact with people online who make me feel uncomfortable
- □ I won't share personal information
- □ I will ask for help with something goes wrong or feels wrong

Create a positive online experience that reflects how you want to be treated

- □ I won't be mean to others online
- □ I will tell someone – like a parent or teacher – if someone is mean to me online
- □ I will check in with my friends if they are upset because of what someone said to them online

Name:

Signature:

*Suggested inclusions only.

Children can be the victim of scams too

Despite growing up with technology, young people are statistically more likely to fall victim to online scams. There's a couple of key reasons behind this.

In childhood and teen years, the brain is developing[3]. The centres that process emotion and reward are highly active, and the part responsible for judgment impulse control isn't fully mature until adulthood. This can lead to over confidence and decisions being made fast and impulsively.

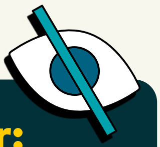
Scammers know this and have become very good at social engineering - that is developing and using tactics – including exploiting platform-specific behaviours - to exploit vulnerabilities across different age groups[4].

Other factors placing young people at risk include greater digital exposure and economic pressure. Life is lived online and over-sharing personal information can lead to unwanted contact or other cyber-criminal activities such as hacking or scams.

Explain to your child that personal information is precious and includes a wide range of specific information about an individual. Sharing personal information online, even in ways that seem insignificant and innocent opens an opportunity for scammers to use it.

Personal information[5] includes:

- ✓ Full name
- ✓ Date of birth
- ✓ Telephone number
- ✓ Address
- ✓ School details
- ✓ Bank account details
- ✓ Commentary or opinions made by or about your child (for example in the gaming chat)
- ✓ Photos (for example that you or your child's school or sports team have posted on social media)



Conversation starter:

If you share a selfie online of you in your new school uniform, there is a logo on your shirt telling the world where you go to school. Can you think of why it might be a good idea to keep that information private?

Did you know?

According to Scamwatch, the top scams for effecting young people under 18 years are shopping, investment and employment scams, with the top methods of contact being online, text and phone call.   Sometimes this can play out in purchasing items that don't exist and never arrive, or having their skins stolen in their favourite game.

There's also more sinister scams that involve blackmailing young people for money or intimate content. Our Gen AI Guide for parents covers this in more detail.

We also know that many young people don't report being a victim of scams for fear of having their device taken away. As parents and caregivers, we should aim to normalise conversations around this type of crime.

Conversation starter:

Hey, I've heard that some other kids at school have tried to buy new avatars but had their money stolen by someone pretending to be another gamer. Have you ever had someone approach you offering to sell stuff for the game? How could we decide if it was a real or fake offer?

[3] Development Decoded. Brains Under Construction: Why Teens Take Risks

[4] RMIT Australia. Gen Z and Millennials are more likely to fall for online scams, despite being more digitally connected.

[5] Office of the Australian Information Commissioner. What is personal information?

Remind your child that it's better to be suspicious and get it wrong, than end up being scammed.

Explain the G.A.P.S checklist to help your child spot a scam.

G

Gain trust:

Scammers might say they are from a legitimate organisation or impersonate someone familiar to make them trustworthy. Check to see if they are who they say they are.

A

Appeal to your emotions:

Scammers know that their targets are more likely to help them if you feel bad for them or really like them, so they might lie about sick pets or family members, or give loads of personal compliments. Acknowledge these feelings but refocus on suspicions.

P

Procedure change:

Scammers will insist on using their own verification procedures, such as sending their target to a new website or phone number. It might feel or look identical to the authentic procedure so refocus on suspicions and stop the procedure.

S

Speed:

Scammers create a sense of urgency to get their targets to make decisions without thinking them through. If they say you need to act now or that the offer expires today, wait until you have done your own research into the offer.

Further reading link:
Protecting your child's identity: Stay ahead of scams

The impact of AI is also presenting challenges. We surveyed over 4,500 students* and year on year, there are significant increases in young people saying they can't recognise if content is made using Gen AI, as well as AI scams and extortion, and deepfakes and chatbots. Young people and criminals are altering photos found online and using them to create explicit content to bully and humiliate fellow students, or, in the case of criminals, blackmail their victim, or their victim's family[6], for money or more explicit content. Our Gen AI Guide for families covers this in more detail.

	2024	2025
Identifying if it's made using Gen AI	13.9%	**32.1%**
AI scams and extortion	12.6%	**22.1%**
Deepfakes and chatbots	9.2%	**15.3%**

* Students participating in the Optus Digital Thumpbrint workshops from DEC 2023 to DEC 2025.

[6] Internet Crime Complaint Center. Criminals Using Altered Proof-of-Life Media to Extort Victims in Virtual Kidnapping for Ransom Scams.

After setting up your child's new device, message notifications are coming in fast.

One message gets your child visibly upset.

New tech often creates excitement, and opens access to new platforms to interact with friends. It can also be a new space for your child to experience bullying, such as exclusion from online group chats in messaging or gaming platforms or mean text-based messages or pics. Role model upstander behaviour that calls out any type of cyberbullying and empowers your child to take action, such as reaching out to the cyberbullying victim to see if they're okay.

Conversation starter:

I can see that that message has upset you. That's not OK for someone to be mean like that, and we should do something about it. Why do you think it's important to do something? What could happen if we just ignore it? Let's work together on a plan for how you'd like to handle it.

Did you know?

Whether it be a nasty comment or a cute kitten GIF, notifications can be super distracting and can have a big impact on study. Notifications and other tech distractions were reported to negatively affect academic performance in **67%** of studies in a recent systematic review[7]. Take action by encouraging your child to turn off notifications during study periods.

[7] Alghamdi, A., & Alghamdi, A. (2025). Digital distraction in education: A systematic review of causes, consequences, and strategies. Educational Technology Research and Development. Advance online publication.

Optimising studies with tech

A device is an excellent tool to enhance learning, but it can also be a distraction. Spend time with your child to explore the features of the device that could assist with focused study time, capturing notes and taking regular breaks.

Activity: "Find the Following"

Together with your child, search you child's device for the following wellness features and spark a conversation about it.

What it is	What it does	What to say
Notifications	Manage alerts from apps and operating systems	Why would it be a good idea to mute notifications on your devices while studying? Is there a time where you might need to enable them?
Screen brightness	Control the amount of light emitted from the digital screen.	Your eyes can easily strain to read the screen if it is too dim in brightly lit rooms, or too bright in darkly lit rooms. Let's discover the range and settings of your screen brightness together!
Focus	Temporarily blocks notifications for a set amount of time to assist in focusing on certain tasks.	Did you know that the brain works better with regular breaks? We can set up a timer that focuses your study for 20 – 30 minutes, then it alerts you to take a 5-minute break.
Notes and document editing apps	Like digital "Post it" notes, notes apps are a quick way to capture your thoughts, to-do lists and reminders. Document editing apps, such as MS Word, Google Docs or Apple Pages are better for bigger projects that need more formatting.	It's a good idea to plan how you want to capture your digital notetaking. Let's explore your device to see what built-in apps it has to help with this.

Did you know...

Almost 4 out of 5 schools are using AI education tools already[8]

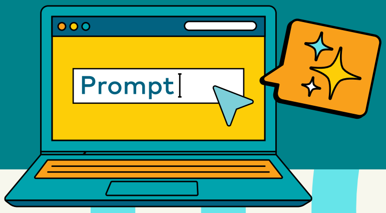
AI vs GenAI

AI is technology that lets devices perform tasks that normally require human intelligence.

Generative AI (GenAI) goes further by creating new content—like text, images, music, conversations, and videos—on its own.

What is a prompt?

A prompt is a written or spoken instruction you give to a GenAI tool to guide it in creating the response you want.



GenAI tools as a study partner

GenAI is a very powerful partner tool that can support learning. The key here is to harness its power and know it's limitations. Guide your child through the following prompt exercise to show them how to get the most out of their GenAI tool.

Steps to prompt GenAI tool	Conversation starter:
1 **Be clear and specific**	What do we want the GenAI to do?
2 **Give it context**	What is the background information, scenario or topic that could help the tool understand your needs better?
3 **Exact requirements**	What do you want the GenAI tool to produce? Such as 5 dot points, 2 paragraphs, an illustration or model?
4 **Regenerate**	Test the prompt out and if needed adjust or refine.

[8] Campion Education. (2025). Digital landscapes in Australian schools: Research report 2025. Campion Education.

Explore our guides and quizzes

Check out these other Optus Digital Thumbprint resources for more information on how you and your child can navigate cyberbullying scams and Gen AI.

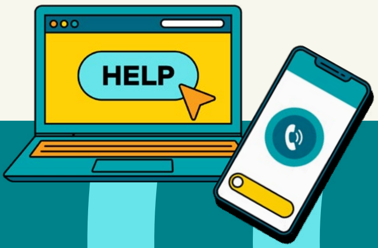
- Cyberbullying – Quiz
- Gen AI and online safety awareness – Quiz
- Cyberbullying: What to say when things go wrong - Family guide
- Cyberbullying: What to do when things go wrong - Tween guide
- Generative AI and online safety - Family guide
- Protecting your child's identity: Stay ahead of scams - Family guide

What to do if your child needs more help

- eSafety Commissioner to report cyberbullying, image-based abuse, and illegal and restricted content
- Australian Cyber Security Centre to report a cybercrime , including online threats and abuse, scams and hacks, data breaches, identity theft and fraud
- Scamwatch to report scams
- IDCARE to get identity theft, data breach, scam and cyber security support

If your child needs to talk to someone about their feelings or worries, they can contact any of these free, private, 24/7 services:

- Kids Helpline on **1800 55 1800**
- 13 Yarn on **13 92 76**
- Lifeline on **13 11 14**



About Optus Digital Thumbprint

Through our Digital Empowerment strategy and programs, Optus is enabling all Australians to achieve, thrive and belong in a digital world.

Optus Digital Thumbprint supports digital safety and wellbeing for young people and families. Find out more at www.digitalthumbprint.com.au

Trusted eSafetyProvider
esafety.gov.au