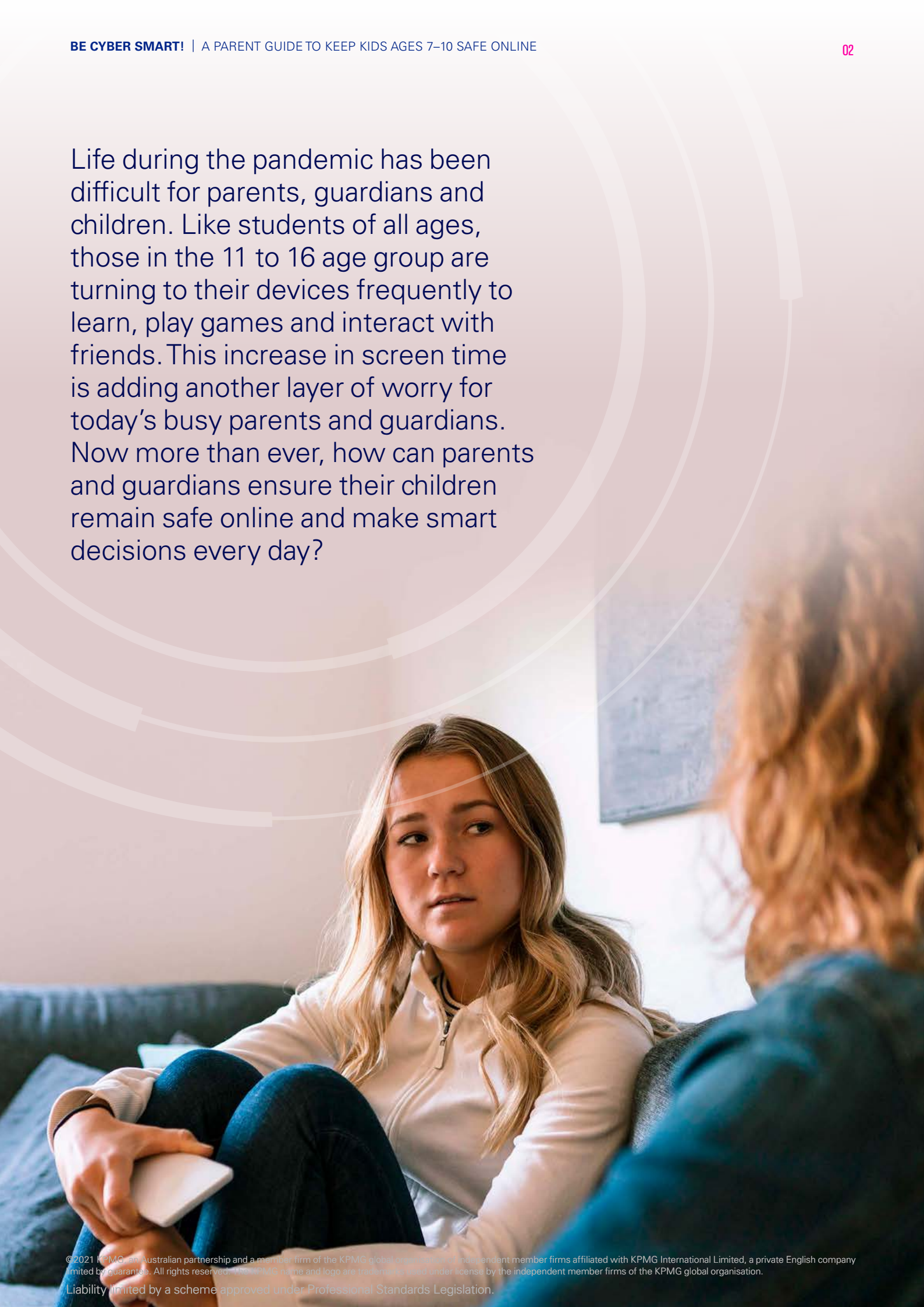
BE CYBER SMART

A parent guide to keep kids and teens ages 11–16 safe online

KPMG

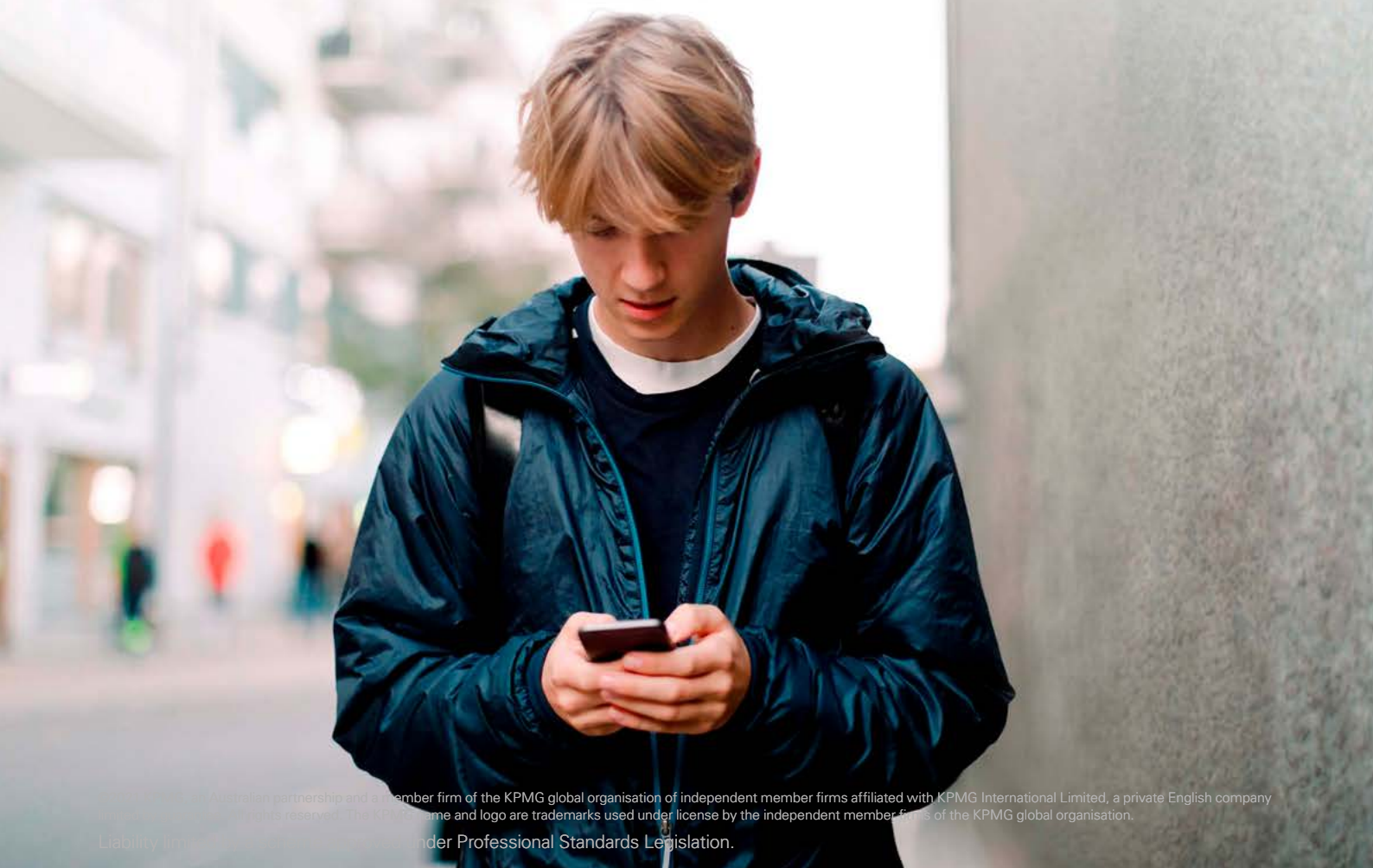
Life during the pandemic has been difficult for parents, guardians and children. Like students of all ages, those in the 11 to 16 age group are turning to their devices frequently to learn, play games and interact with friends. This increase in screen time is adding another layer of worry for today's busy parents and guardians. Now more than ever, how can parents and guardians ensure their children remain safe online and make smart decisions every day?



Stay involved and always keep safety top of mind

The internet is a wonderful resource when used safely. Be honest and open and build trust, explaining why it is very important to be careful whenever online.

- Demonstrate and stress how to use secure passwords, how to identify secure webpages, how to spot scams, what appropriate online behavior looks like and other skills for online safety.
- Review your child's internet activity and social media accounts regularly.
- Ask questions and encourage open dialogue about what they do online, the sites they visit and who they talk to.
- Practice what you preach by setting a good example with your own online presence.



How to stay cyber smart!

Six helpful tips to keep kids and teens 11 to 16 safe.

1 Manage screen time wisely.

Ever-present computers, tablets and phones can lead to excessive screen time that is harmful. Overuse can lead to what doctors call 'screen dependency disorder'. Be careful — physical or mental health can suffer. Screen time beyond schoolwork ideally can be allowed after homework is done or during free time on weekends.

2 Keep it to safe chatting activity at all times.

Warn against chatting with any strangers and offer help to block messages from anyone who is unfamiliar. Stress that sharing images, personal information or messages that are offensive is wrong. Teach kids and teens the difference between public and private chat rooms.

3 Always keep personal details confidential.

Your child should never share details such as their full name, home address, passwords, location or phone numbers with anyone they don't know via texts, social media, online gaming, etc. Stress the need to keep all personal information safe and to create different passwords for every online account or use a password manager. A password manager will allow you to store, generate and manage your passwords — minimising the number of passwords you have to remember. Suggest to your kids to only remember three passwords: one for school, one for their computer and one for their password manager — with all other passwords being stored there.

4 Friends only please..

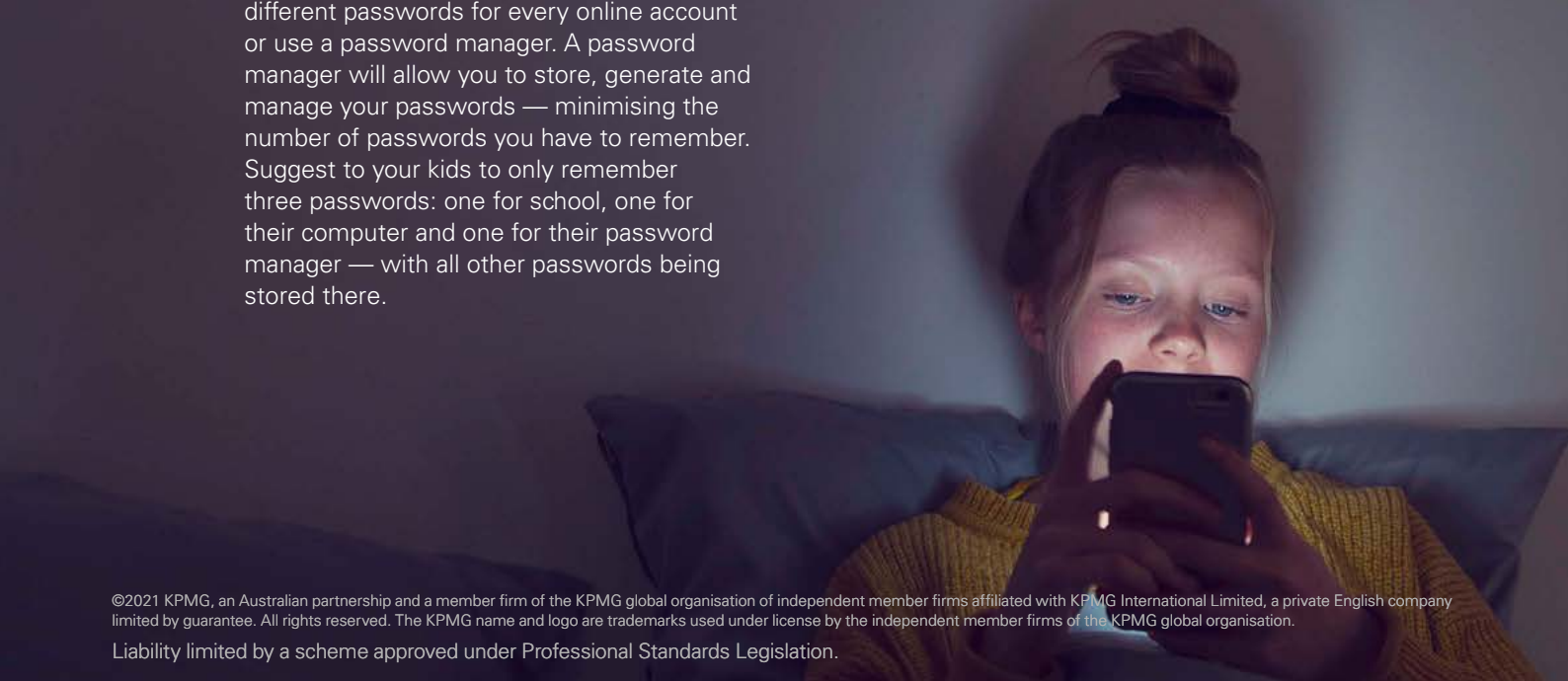
Be aware of the risks of interaction with strangers through social media, discussion boards, online gaming, texts, etc. Kids and teens tend to be very active socially. Warn them against meeting anyone in person without your knowledge and consent. Help to arrange a safe way to meet new friends and set a specific time and place.

5 Check it before you click it.

Children should never click on links in emails unless from a familiar source or open any attachments that have come from an unknown sender. Note that any organisation or institution will never request their personal information by email. Do not reply to spam emails and warn against visiting websites that they do not trust or know.

6 No one likes a bully.

Discuss bullying openly and advise your child to report all negative comments to you. If you suspect cyberbullying, encourage open communication so they feel comfortable telling you what's going on. Also, remind them to be careful about what they say, share or post about others — unintentional bullying is still bullying.



'Play it smart' when gaming

While online gaming can provide hours of entertainment and social connection, there's also a darker side. From cyberbullying to online predators to hidden costs, there are many concerns when it comes to playing video games online. Here's how you can help protect your kids and teens:

- Discuss and determine which games are appropriate for children and teens ages 11 to 16.
- Ensure that they know what conversations are acceptable if gaming with strangers. Encourage gaming with friends if possible.
- Set expectations and rules for time limits and allowed games.
- Ensure they understand what personal information is and the importance of never sharing it while gaming or online.
- Reinforce all gaming rules regularly.

Tips for social media safety

There are plenty of good things about social media — but also many risks that kids and teens should avoid. From predators to cyberbullies, their misuse of a social media can have serious consequences. Here are some tips for how you can keep your kids safe on social media:

- Most social media sites have age restrictions. Ensure and monitor compliance.
- Encourage your child to stop and think before posting comments or pictures and to never share personal information like their age, school, address or full name.
- 'Friend' or 'follow' your child online to oversee social media activity. You don't have to participate, just view profiles and posts regularly.
- Review social media parental guidance pages and work with your child to apply the security settings that best protect their privacy.
- Data provided to social networks is stored and often shared by default. Ensure your child's profile is set to 'private' mode. Review all account settings together.

Cyberbullying

Cyberbullying is a form of bullying using electronic forms of contact and has become increasingly common. Though similar to regular bullying, cyberbullying takes the trauma one step further by allowing aggressors to follow the victim wherever they go. Virtually anyone, anywhere, anytime can bully another person by simply jumping on the internet or using a cell phone. Here's how you can help:

Communicate

It's crucial today to talk to children openly about cyberbullying.

Educate them to:

— Report offensive or hurtful comments to you immediately, whether they are the target or not.

— Be careful what they say, send, post or blog about others — unintentional bullying is still bullying.

Take action

It´s important that parents and kids take action by:

— Saving bullying texts, posts and emails.

— Not replying and not deleting them.

— Reporting the ID online and blocking the user from further interaction.

— Escalating the issue to your child's school or the police as necessary.

Recognise

Watch for these signs of being cyberbullied:

— Showing unexpected anger, depression or frustration after using any device or avoiding device use all together.

— Uneasiness about going to school or participating in group or team activities.

— Abnormally withdrawing from friends and family members.

Logging in and out securely

Keeping track of passwords can be a hassle. Still, passwords remain the first line of defense against an invasion of privacy that can affect safety both on and offline. Here are a few tips that can help kids log in and out securely.

Choose usernames wisely

— Avoid using a full name, age, address, date of birth, gender or other personal information.

— Advise children to consult with an adult to create usernames if in doubt.

Practice password safety

— Show kids how to combine phrases, numbers, symbols and uppercase and lowercase letters.

— Stress never to repeat or reuse passwords and to never share a password or provide it if requested.

— Avoid passwords that are easy to guess such as a birthdate or favorite sport or activity.

— Try using a password manager and suggest to your kids and teens to only remember three passwords: one for school, one for their computer and one for their password manager — with all other passwords being stored there.

— Remind them to always log out when leaving a site or platform.

— It's best to avoid free WI-FI and the risk of data theft by hackers.

— When visiting websites on updated phones don't enter usernames and passwords.

What can you do?

Be a proactive parent!

Be involved every day — manage internet access and monitor activity

— **Being aware**, staying involved and maintaining close communication can help keep children safe when using the internet. Innovative control tools built into devices and Wi-Fi routers are easy to use and it pays to become familiar with how they work and how to keep them updated.

— **Parental controls** can be used to protect your child from accessing inappropriate websites and can be applied to your network or individual devices. Be sure they are enabled.

— **Logging and monitoring** of your home network lets you review your child's internet activity to ensure safe habits. Take time to openly discuss which websites are appropriate for their age.

— **Schedule internet time** to manage your child's online activity to pre-determined times such as after homework or on weekends. Explain why this is a smart approach to safety.

— **Antivirus tools** can serve as the last line of defense to help protect home computers and devices from dangerous viruses and other types of malware that are becoming all too common today.

— **Back up important information** as data gets lost. For anything really important, keep a copy somewhere else, like a USB stick. For anything that needs to survive more than five years, print it out.

Additional info and resources for the 11–16 age group

By being well informed about online safety, encouraging safe practices and staying involved and aware, parents can better educate kids and teens to practice internet safety.

The following online resources can be helpful in educating children on safe online habits and how to be cyber smart:

Australian Government eSafety Commissioner:
https://www.esafety.gov.au/educators/classroom-resources

Australian Government Online Safety
https://info.australia.gov.au/information-and-services/public-safety-and-law/online-safety

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

KPMG Global Cyber Day:
KPMG.com/au/cyberday

October 2021. 759392318FIRM