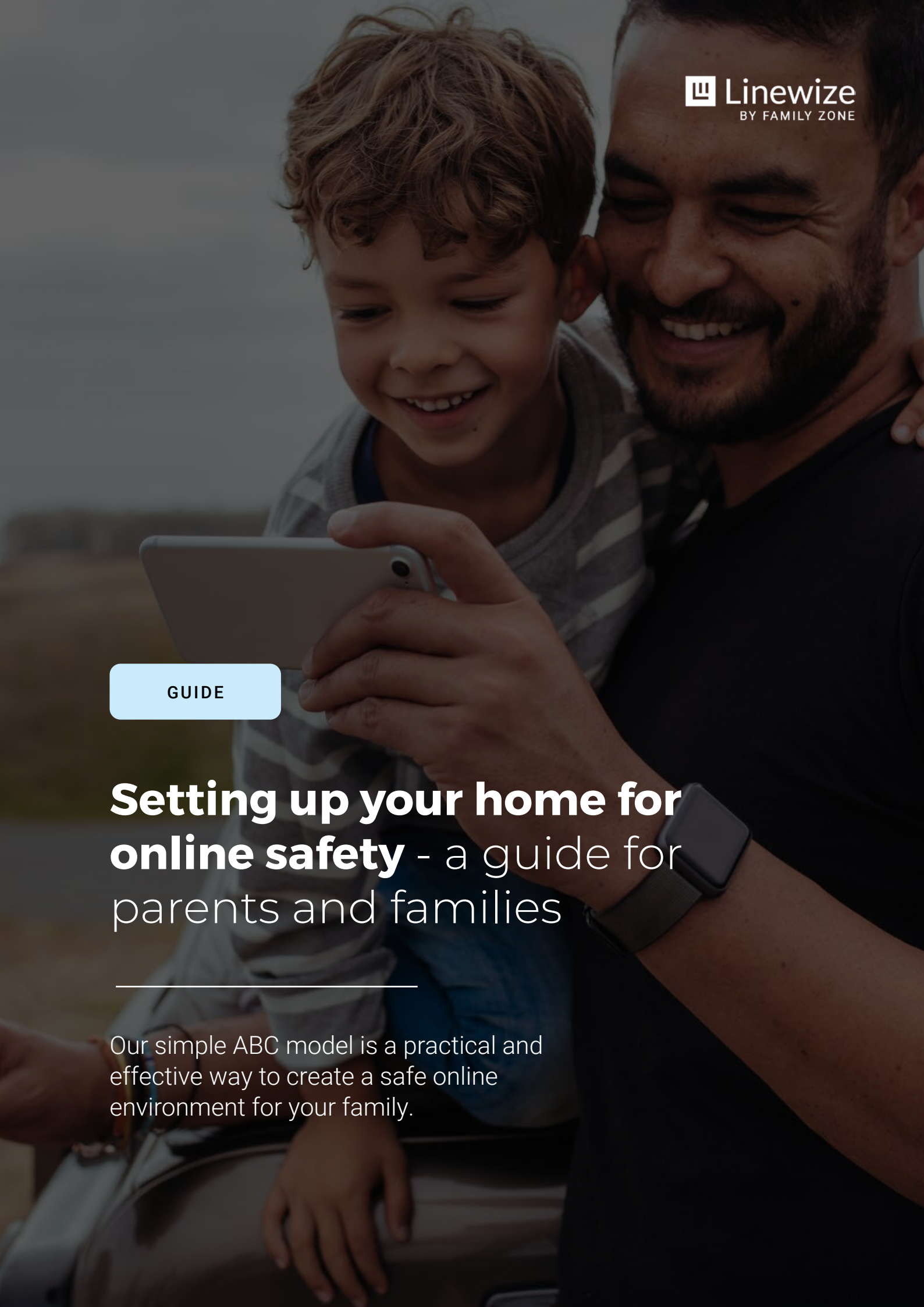

Linewize
BY FAMILY ZONE

GUIDE

Setting up your home for online safety - a guide for parents and families

Our simple ABC model is a practical and effective way to create a safe online environment for your family.

Setting up your home for online safety - a guide for parents and families

Our model of setting up a cyber-safe home involves three key steps. We call this the ABC model, involving safe access, clear boundaries and communication. By following the model, parents can create a digital environment that not only protects kids online but helps them thrive. Below, we have outlined the goal for each step and practical suggestions on how to achieve them.

Control **Access**

Before giving your child access to a device, it is essential that the device is set up to be safe for the child's use. Think of it this way- you wouldn't give your child access to a car without brakes and a seatbelt, why would you give them a device without filtering and privacy settings? Setting up a device with safeguards is an essential step in creating a cyber-safe home. Controlling access allows parents to control what kids have access to and when they have access to it, always ensuring that access is safe.

01 Apply manual safety settings on all devices (ages 0-9) OR use parental control tools to block access to age-inappropriate apps and manage screen time (ages 10-16).

02 For primary-aged children, turn on Google Safe Search and YouTube Restricted Mode on each device.

03 For secondary-aged kids, have a strict 'off' time at night time. Use parental control tools to block access to social media and entertainment apps after bedtime.

04 Ensure access to social media and gaming apps is safe by turning on Privacy Settings and turning off Geolocation for apps where it is not essential.

05 For primary-age children, set up all apps and accounts with a parent's email address and password (and don't tell your children the password!).

Quick Screen Time Wins

- Turn off all screens during family meals and outings.
- Keep devices in public areas (rather than in the bedroom).
- Turn off devices 30-60 minutes before bedtime.
- Ensure screen time is balanced with other activities such as sleep, social activities, reading, and hobbies.

access

Set **Boundaries**

Setting boundaries is about establishing clear rules and expectations about how kids use their devices. This is vital in helping guide children and teens to develop positive digital behaviours. Without rules, children and teenagers are left to their own devices (pun intended) to decide what they should do online and when they should do it. Boundaries are essential not only for supporting kids' well-being but for helping parents teach their children between right and wrong. Reinforcing those boundaries when kids don't follow them is also just as (if not more) important than the boundaries themselves. Expect rule-breaking; it will happen. But correcting behaviours and reinforcing rules will pay off in the long run.

01 Use a Digital Contract (a written document for ages 3-14, a verbal agreement for ages 15+) to set clear rules about online behaviours. Include rules about appropriate ways to communicate online and what role you are taking as a parent in their digital lives (e.g. will you be following their social media accounts?).

Tip: Getting kids to co-develop the contract is a great way to get their buy-in.

02 Reinforce rules when they are broken. Jot down positive and negative consequences. Many parents just use negative consequences for bad behaviour, but having positive consequences for good online behaviour reinforces learning much quicker. If you've jotted them down before you need them, then it's quick and easy to reinforce behavioural consequences when you need them.

03 Set up a Screen Time Schedule. Having clear boundaries around time online helps with decreasing kids' obsessions with technology, as they clearly know when to expect it. For primary-aged children, this should be very structured (eg. leisure time on their device between 4-5 pm each day). For teenagers, this should be very clear 'off' times (eg. no screens after 9 pm, no social media use during homework time - you use a parental control tool to enforce this).

04 Adopt a screen-free area or screen-free time in the house. This allows open conversation between the family and digital downtime. The important point here is that the area or time needs to apply to everybody in the home, including parents. Modelling is an essential part of cyber safety education.

05 No devices in bedrooms. Cyber safety risks increase late in the evening due to feelings of privacy and safety. In addition to this, a part of a child's brain that regulates their behaviour isn't fully developed until they are 25. So expecting kids not to touch their gaming consoles while they are supposed to be sleeping is setting them up to fail.

boundaries

Openly **Communicate**

Teaching kids about cyber safety is central to helping kids thrive in the digital world. Research has highlighted that children and teenagers predominately learn about cyber safety either from their friends or from Google. Information from a healthy, responsible adult is the only antidote to this. Cyber safety should be a regular talking point in every household to protect kids online.

01 Get involved in your child's digital life. To effectively communicate, you need to know what apps and games your child is using. Then, you can tailor cyber safety messages to address what they're facing online specifically. Ask your child questions often, and enquire what they like about their apps and games. Be sure to make the conversation positive (not demonising technology!) to promote their engagement in the chat.

02 For primary-aged children, the key learning points for them are online strangers, catfishing (people pretending to be someone they aren't), personal information, and privacy. Conversations about not being able to control where your information and pictures go (along with privacy settings on) are helpful too.

03 For secondary-aged children, the conversation is much broader. They need to learn about cyberbullying and dealing with online conflict, technology-related laws, the risks of sending nudes and peer pressure, excessive technology use, digital footprints and their online reputation.

04 Use stories and anecdotes to help kids learn. This is helpful because not only do humans remember stories easier than facts, but a story about someone else can feel less confronting for a child than simply telling kids what to do and not do.

05 Debunk the myth for children and teens that you will take their devices away as a safety precaution if they tell you something has happened online. Only 1 in 10 young people let their parents know if they are being cyberbullied online due to fear of having their social media or device removed. Be sure to let your children know that this won't be the case, and they should always come to you with their concerns or challenges because you'll help them find a thoughtful solution that works for them.

communicate.

About Linewize

We empower school communities to guide students towards safe and positive behaviours in their digital lives. When students know how to stay digitally safe and well, their confidence grows, their resilience increases and learning improves.

We combine safeguarding technology, child psychology expertise, indepth educational material and awareness initiatives to help schools build positive digital cultures - where students can thrive.

As the digital landscape has evolved, so have we. From our humble beginnings in user authentication and content filtering we're now part of one of the biggest digital safety and wellbeing providers in the world. 23,000 schools and 12 million students rely on our technologies and educational programs everyday.

Our goal is to work together to save and better children's lives; empower parents; deliver for tomorrow's educators and to be a key influencer in digital safety globally.

Linewize
BY FAMILY ZONE