10 Top Tips for Parents and Educators
USING AND REVIEWING PARENTAL CONTROLS

Phones and computers are essential parts of children's lives, but with unfettered internet access comes a multitude of risks. While not foolproof, parental controls can help with this; filtering out inappropriate content, limiting the ability to spend real money, capping screen time and generally making devices safer for young people.

1 KNOW THE TYPES

While parental control software can apply to an entire device, it also pays to know about options on individual apps and websites. TikTok, for example, has Restricted Mode for limiting unsuitable videos, while Snapchat lets you keep an eye on who a child has been talking to. Check the settings of any new app young users want and review your options.

2 COVER ALL DEVICES

Knowing what parental controls cover is crucial, as remaining unaware can run the risk of 'blind spots' in the device's safety measures. Controls on a phone will apply whenever a child's on that device, for instance – but you'll want to ensure that parental controls are set up across any laptops, tablets and potentially other phones, too. Remember, buying a new device may require you to set everything up again.

3 DON'T NEGLECT SHARED TECH

While children often have their own devices, if you have a shared family computer or tablet, for example, you'll need to make sure that's not a weak point in your safety measures. Parental controls for your router, that cover everything connected to your Wi-Fi, are one option – or you can just be thorough with each device and online account. Just ensure that unprotected laptops, phones and tablets are password locked.

4 CONSIDER TIME CONTROLS

Even safe internet content can be harmful if it's viewed in excess. Not only are certain apps addictive enough to distract from other duties, but late-night usage can badly disrupt sleep, which is vital for adolescent brain development. Most parental controls offer some kind of time limit – either blocking access at certain hours or capping the number of minutes it can be used per day – so be sure to consider these.

5 BLOCK APP SPENDING

Seemingly free apps can sometimes include microtransactions: purchases that can be made using real money. While plenty of developers implement these fairly, some companies attempt to manipulate children into paying for additional features or content, which can soon add up to hundreds of pounds if a child gets carried away. Thankfully, iOS and Android's settings allow you to block in-app purchases, preventing any huge bills.

6 NO CONTROLS ARE PERFECT

Parental controls can be very useful, but they're far from infallible. Some unpleasant content can and unfortunately *will* slip through the net, so remember that setting up these measures isn't a substitute for taking an active interest in young people's digital lives. Talk to them, and make sure they're aware of the risks of the internet as well as its benefits.

7 MIND THE GAPS

There'll undoubtedly be *some* gaps in parental controls, no matter how thorough you intend to be. For example, if you use router-level parental controls, bear in mind that these won't cover WiFi outside the home. For that reason, it's important to keep an open dialogue with children about the many unpalatable aspects of social media and the web.

8 KEEP THINGS SECURE

Some children can react poorly to parental controls and feel tempted to circumvent them. It's important to ensure that the passwords to these settings remain unknown to children, otherwise they can easily modify the restrictions without you knowing. Similarly, make sure your phone isn't left unlocked and unattended.

9 REVIEW CONTROLS REGULARLY

Parental controls shouldn't be a 'set and forget' deal. Not only can parental summaries provide you with a frequent overview of a child's digital life – to let you spot any warning signs – but companies often add new features, and some of these may be useful to enable (or disable). Regularly checking in ensures that if a child *has* found a way to wiggle out of the controls, you'll be the first to know.

10 KNOW WHEN TO LET UP

The parental controls you install on a computer for a seven-year-old probably wouldn't be appropriate for a child of 16 — and as young people approach adulthood, bubble wrapping the internet can do more harm than good. Consider relaxing parental controls as children get older, so they can learn to manage the risks of the internet themselves, without so many training wheels.

Meet Our Expert

Alan Martin is an experienced technology journalist and the former deputy editor of technology and internet culture website Alphr. Now freelance, he has contributed articles to publications including the New Statesman, CNET, the Evening Standard, Wired, Rock Paper Shotgun, Gizmodo, Pocket Gamer, Stuff, T3, PC Pro, Macworld, TechRadar and Trusted Reviews.

#WakeUpWednesday®

The National College®