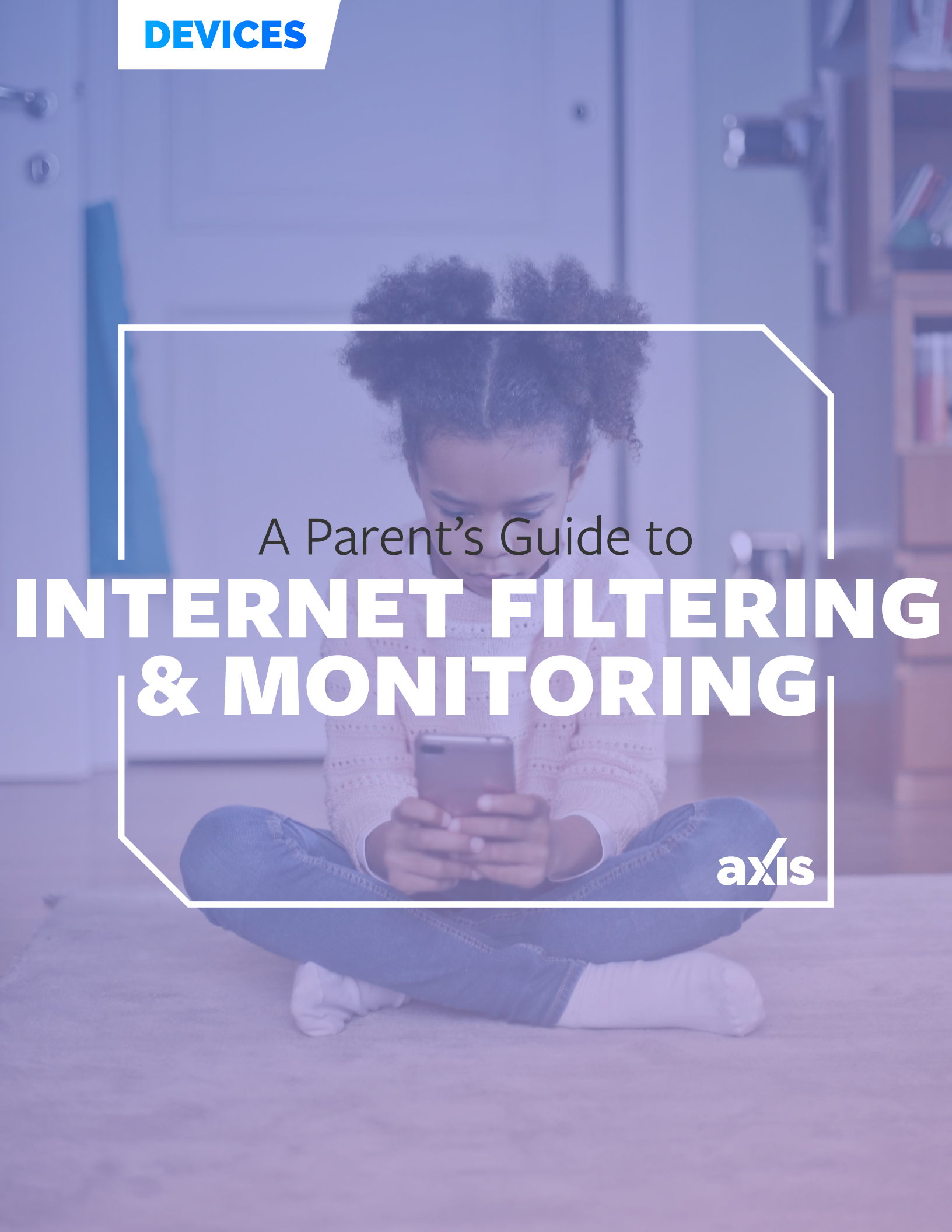
DEVICES



A Parent's Guide to

INTERNET FILTERING & MONITORING

axis

A special thanks to Canopy,
a digital parenting app, for sponsoring
this Parent Guide.

> “Your ultimate goal is to raise kids who use the Internet safely and responsibly and think critically about their actions, but a little technical assistance can help. And, as your kids get older, you’ll need to dial down the restrictions to help them develop their own sense of responsibility.”
>
> —Common Sense Media

A Parent's Guide to
INTERNET FILTERING & MONITORING

Contents

axis

Monitors and filters are useful, but they shouldn't replace relationships.

There's no question that there's a lot of filth on the Internet. And it's pretty easy to bump into. Sean Clifford, CEO of the digital parenting app Canopy, notes, "You don't have to go looking for [porn], it now comes looking for you. It's on social media, on group chats, and on 'good' websites that you'd never expect to have explicit content." A recent survey found that 46% of minors who've seen pornography first came across it by accident.

Internet filters are extremely useful tools in a world where inappropriate content seeks us out. But we shouldn't use them as a replacement for relationships and conversation; as a friend of ours wisely said, "Setting up a filter on your child's device is a great moment for a conversation."

In the same way that sending our kids to Christian school won't automatically make them Christians, setting up an Internet filter won't always protect them from graphic content.

We hope that parental controls are just one part of your overall strategy for protecting your children. Don't view Internet filters as final solutions. Instead, view them as first lines of defense that should be paired with intentional discipleship, encouraging our kids' hearts to want what is good and to hate what is evil.

Why aren't filters enough?

It makes sense to long for a bulletproof solution, to want to create an environment where our kids will never encounter graphic content (by choice or by accident). But filters alone are not a perfect safeguard, for many reasons:

- **We simply cannot control every place where they might encounter porn.** As David Eaton, Axis' co-founder, puts it, "Your kid is only as safe as their friend's phone."
- **Apps (as opposed to websites) can't be filtered.** And pornographic content can be available in seemingly safe apps (Libby, the library app, has erotica and romance literature that can be classified as soft-core porn).
- **Teens are tech-savvy.** And if they're determined, they can find ways around the boundaries we implement. How? These are just a few creative ways kids might bypass parental controls.

- **Internet filters can provide a false sense of security.** A friend of Axis told us that some teens ask their parents to install specific filters under the guise of working through their porn addiction, when in reality they know how to bypass those filters. Pretty sneaky. We're not saying that all teens are this manipulative, but it is good to remember that teens are digital natives (we are digital immigrants), and good to assume that we're probably always a few steps behind their tech savviness.
- **We can't filter our kids' worlds forever.** They will grow up, so we need to teach them how to be responsible adults, not try to shelter them forever.

Don't get us wrong—we think Internet filters are great, especially as one part of an overall strategy to avoid graphic content. We think that every family should find the internet filter that's right for them. In the same way that seat belts are necessary safety measures (even though they can't guarantee your teen driver's safety) internet filters are essential guard rails. We just can't fall into the trap of thinking that getting one is a one-time, catch-all solution.

Because there's no silver bullet to keeping our teens safe on the road or on the internet, we should put up defenses where we can, while also educating our kids about Internet safety, talking with them about the challenges of interacting with people online, and starting the conversation about porn before porn starts it with them behind our backs (see our resources about pornography for more information about how to do so).

What's the difference between Internet filters, Internet monitors, and parental controls?

Though the terms are often used interchangeably, for the purposes of this guide, we'll use them to refer to different things.

Parental controls refer to the built-in controls on a device that restrict access to content. These articles from Canopy give step by step instructions for using parental controls:

- "How Parental Controls Can Help Protect Those You Love Most"
- "5 Tips for Talking with Your Kids About Parental Control Apps"
- "How to Set Up iOS Parental Control (Apple)"
- "How to Set Up Android Parental Control"

Other devices, like gaming consoles and tablets, often come with (limited) parental controls.

Internet filters are third-party software or hardware that restrict access to online content.

Internet monitors are third party software or hardware that record someone's internet activity and usage, and then deliver a report that details sites visited, time spent online, etc.

What's the best strategy for implementing filters and monitors?

Using Internet filters and monitors is like teaching a teen to drive. They aren't good to go at 16. First, they need a permit (which requires learning information about driving before getting behind the wheel), hours of supervised driving to gain experience, and even after they get their license, they need rules and boundaries until they have a few more years of experience ("Text me when you get there!" "Home by 11pm, please.").

As they mature and become more capable, we slowly remove some of the boundaries and trust them to be discerning until they move out on their own.

Though Internet filtering is newer territory than teaching our kids to drive, we should approach it similarly. In an ideal situation, the best strategy for protecting our kids online would start with strict parental controls, internet filters, and monitors when they're young and first using devices. As they get older, we would continue to have formative conversations with them about things like social media, cyberbullying, and pornography, and then slowly reduce the strength of our filters and Parental Controls while continuing to monitor their activity, letting them earn more privileges and responsibility. And if they prove not to be trustworthy, these privileges would be revoked.

If we've done our jobs properly, when they leave home for the "real world" they will be prepared for total internet freedom while understanding how necessary continued submission to accountability is in our tech-saturated world.

Sounds great, but my situation is definitely not "ideal." So what do I do?

No situation is actually ideal when it comes to the Internet and technology. Everyone is trying to figure out how to navigate this ever-changing, constantly connected world, and thus far, there's no step-by-step manual for success. No matter how old your children are or how much you feel like you've "messed up," it's never too late to start introducing technology accountability into your home.

If your kids are older, start by having conversations with them about what you'd like to implement. Explain why, and let them ask questions and express frustrations. Here are a few talking points to help this conversation go more smoothly:

- **Get their input and ideas first.** Consider saying: "We're thinking about ways to use technology more intentionally as a family. Part of this will probably look like installing an internet filter, and we're trying to think of some other ideas as well. We want to get your input about what would be most helpful for you." Then ask a few questions:
    * "What do you think makes sense?"
    * "What do you like about the ways we currently use our phones/technology as a family?"
    * "What would you change about the ways we currently use our phones/technology?"
    * "Have you ever wished you could log off more easily from a given app, or that you spent less time gaming, on social media, or on your phone?"
    * "How can we create boundaries that actually help you do what you want to do?"
- **Be in this with them.** Make it clear that the accountability will be for everyone in the home, including you (not just them!). If you want them to spend less time on social media, implement the same limit on your own social media use. If you're checking their photos or Instagram account, give them access to your photos and Instagram account. If you expect them to have nothing to hide, make it clear that you have nothing to hide (and that accountability is good for everyone, both teens and adults).
- Try to make it clear that **you're on their side** and want to help them truly flourish, not be the bad guy.
- **Give them quick and clear ways to gain privileges/responsibility** (like increased privacy, more screen time, more time on specific apps, etc.). The goal is responsible tech use after they leave your house. Since they're older, complete tech freedom is coming soon.

They may be angry at first, but if done well, they may eventually come to see that boundaries are good for them (if they continue to be angry, it may be because there's already something they don't want you to know about. If that's the case, then you know you're actually on the right track).

Once you've had the conversations with them, figure out what's age appropriate for each of your kids (some may still require lots of filtering, while others are mature and should have monitoring and accountability instead). Then slowly begin introducing the new systems into your home.

What do I need to know before deciding on an Internet filter?

While we definitely disagree with the LDS Church's theology, their article about Internet filters is a great resource for getting a basic understanding of the ways that filters work. It's helpful to understand what types of filters are out there so that you know which are the best solutions for your family.

From a technical perspective, there are three ways to filter the internet:

- **Blacklist / whitelist** - only allow kids to go to specified websites (whitelist) or stop kids from going to specific websites (blacklist).
- **Text-based analysis** - The filter reads the webpage and blocks it if the text appears to be inappropriate.
- **Image-based approach** - The filter looks at every image and determines if it involves nudity.

There are also three levels at which you can filter:

- **ISP-level.** Many internet service providers (ISPs) allow you to request for your home to not have access to pornography. Not all ISPs offer this, and their filters can be outdated and easy to circumvent. This is filtering at the level of the pipe before the internet enters your home.
- **Router-level (hardware).** Some services allow you to filter your internet at the router level. While the pipe carrying the internet into your home could bring in porn, it would be stopped at the machine that creates your wifi.
- **Device-level (software).** This creates a filter on the device itself (phones, computers, iPads...) so that even with unprotected internet access (think: your local fast food joint's WiFi) your child is still protected. This can't be

circumvented with different WiFi or a different ISP.

The majority of filtering solutions are types of software. Software-based Internet filters tend to have the most variety of features and the greatest capacity for customization.

We would argue that device level protection (software) is a really good idea, while router and ISP filters (hardware) are wise secondary layers of defense (since hardware solutions can be easily bypassed by using cellular data or a different WiFi network).

Some solutions work through a VPN (virtual private network). Internet filters that work through a VPN filter content through their own networks, as opposed to filtering via ISP, router, or device (but beware: just as we can use VPNs to filter content out, our teens can easily learn how to use VPNs to get around filters).

Before deciding which filter you need:

- Decide which devices you want to protect. If you're concerned about devices at home, you'll probably want to focus on something that filters every device through your WiFi.
- Remember that you can combine filters; you can protect specific devices with software filters while also protecting your home WiFi with a router-level solution (so even if your teen's friends have filterless phones, they won't be able to easily access porn while using your WiFi. But remember, they can hop off WiFi and use data instead, so this isn't a perfect solution).
- If you go with a software solution for individual devices, remember that it might not be able to protect every Internet-aware device you have in your home if your kids have iPods or gaming consoles.
- Your operating system impacts your choice of filter. While we'll try to recommend filters that work with a variety of operating systems (see below), parental control solutions usually favor certain systems over others.

As a side note, some operating systems have protections already built into them, and it would be worth your time to explore these. For example, Apple has features for setting up parental controls on its devices.

Check out this article for good habits for protecting your privacy online. Also consider using Google SafeSearch, a tool Google created to block explicit content online. It's not infallible, but it is somewhat helpful for catching objectionable content.

What are some criteria for good filters?

- Content filtering. Does the filter distinguish between different categories of content? How in-depth is this analysis? Some solutions go so far as to scan pages in real time, allowing certain pages on a site, but not others.
- A detailed and clear activity log.
- Is it browser independent, meaning that it will filter content on any browser someone uses (Safari, Chrome, Internet Explorer, Firefox, etc.)?
- Will it filter content if your child tries to use an anonymous proxy server?

What about online games, smartphone apps, videos, social media, chat, or email? Certain solutions have the ability to filter these types of content, while others don't.

Some filters are so thorough that you can set them up to take periodic screenshots and record keystrokes. While this capability is impressive, when it comes to older teens we caution against being too invasive. It may be more effective to implement a slightly less intense filter and focus on having conversations with them.

Many solutions come with the ability to set time limits and to whitelist (allow) and blacklist (ban) specific URLs. Many Internet filtering solutions also offer a way to track and limit children's locations through geolocation and geofencing. "Geofencing" means setting up a perimeter in a certain area, and if your children go outside those boundaries, you get an alert.

What filtering and monitoring software do you recommend?

In the following list, we want to highlight what we think are some of the most helpful solutions currently available. Keep in mind that our list is not exhaustive, but will hopefully help point you in the right direction. We've also prioritized those that encourage accountability through relationships. Keep in mind that Apple controls its devices more tightly than Android does, so it's normal for a solution's iOS capabilities to be somewhat narrower.

For the following seven recommendations, we've relied heavily on these reviews from PC Mag, as well as information from the companies themselves.

CANOPY

We'll let Canopy's CEO, Sean Clifford, explain what Canopy is about:
"Canopy is a tech company on a mission to create a world of healthy tech users. We think the Internet is amazing, but recognize that it isn't always safe for children. Our first product is a next-generation Internet filter that protects kids from online pornography, wherever it appears."
The Gospel Coalition explains why Canopy is unique among internet filters:
"Many of the most popular websites feature a mix of appropriate and inappropriate content—Snapchat, Facebook, Twitter, etc. It just is the nature of the modern Internet...In this kind of world, the all-or-nothing approach of blocking or allowing entire websites just doesn't work. Only Canopy allows users to filter content within websites. Canopy will allow you to view appropriate content on those sites, while filtering out what's inappropriate."

PROS

- Strong content filtering. Canopy developed artificial intelligence to filter within websites, allowing good content and blocking graphic content.
- App and website blocking
- Location tracking
- Sexting deterrence
- Removal prevention: Canopy can prevent a child from deleting the filter without their parent's permission.
- Hack-resistant: Canopy works with teens to find and stop the workarounds that enable kids to hack through other filters.

CONS

- Like other filters, Canopy doesn't work inside social media apps (think TikTok, Instagram, Snapchat, or Facebook) but it still filters every website (like instagram.com or facebook.com). Parents can block apps they think are unsafe
- Doesn't currently work on Kindle devices, gaming consoles, Chromebooks, or Apple TV.

PRICING

Sign up using the discount code "Axis" to get 30 days free and 15% off forever!

Basic, 3 devices	$7.99/month
Family, 5 devices	$9.99/month
Full House, 10 devices	$15.99/month

OTHER INFO

Canopy is more of a filter than a monitor, meaning that it keeps your child from seeing inappropriate content in the first place, rather than sending you reports of what websites they visit or how much time they spend on their device.

QUSTODIO

Qustodio is one of the most solid Internet filters on the market and appears to be highly recommended by just about everyone who reviews it.

PROS

- Filters inappropriate content (with a lot of customization. You get 26 filter categories and several response options, from blocking the whole page to getting an alert that your teen is trying to access something that you've flagged).
- Detailed activity log. Weekly or monthly reports of your teen's activity and screenshots from their devices.
- Can block content on most internet browsers (Chrome, Safari, Edge, Firefox, and Amazon's mobile browser)
- Extremely customizable time limits
- Location tracking

CONS

- Doesn't block access to VPNs
- Doesn't closely filter/monitor TikTok, Snapchat, Instagram, or other popular social media apps. The only option is to block those apps entirely.
- Doesn't work for gaming consoles or Apple TV

PRICING

Small Plan, 5 devices $54.95/year	**$54.95/year**
Medium Plan, 10 devices $96.95/year	**$96.95/year**
Large Plan, 15 devices $137.95/year	**$137.95/year**

CIRCLE

Circle offers several parental control products. We recommend at least using the Circle Home device in conjunction with the companion app Circle Go. Circle Home is a device you install that will filter all of the devices in your home, but Circle Go will protect your kids' devices when they leave the house. Note that Circle Home doesn't replace your router, but rather works with it.

PROS

- Content filtering by category, browser independent, blocks anonymous proxies, doesn't overblock, protects all devices in the router's network
- Detailed activity log
- Has time limits, internet pause, focus time, and bedtime options
- Location tracking
- App blocking

CONS

- Circle Go doesn't work for laptops
- Circle Go is easy to disable, but you'll be notified
- Can't use Circle Go without Circle Home

PRICING

$129 per year
$329 lifetime

OTHER INFO

Note: Circle Home filters any device connected to your WiFi. Circle Go manages iOS and Android devices, along with many Chromebooks, but does not manage laptops outside the home.

KASPERSKY SAFE KIDS

Kaspersky Safe Kids is a well-rounded and affordable option.

PROS

- Content filtering by category, option to warn about content instead of just blocking it, evaluates web pages on a case-by-case basis, blocks anonymous proxies, flexible options for limiting Internet access, real-time alerts
- In-depth activity log
- Time limits
- App monitoring and blocking
- Monitors games on iOS
- Location monitoring and geofencing
- Unlimited devices and profiles (good for large families and families with lots of devices)

CONS

- App filtering doesn't work on iOS devices
- Filtering doesn't work in all internet browsers
- Limited social media monitoring

PRICING

$14.99/year, unlimited devices and child profiles

NORTON FAMILY

Norton Family is an affordable solution with a wide range of features. We also love that the company encourages parents to have open and ongoing conversations with their kids.

PROS

- Content filtering by category, has customizable options
- Detailed activity log
- Time limits
- School Time feature helps kids focus when learning at home
- App and messaging tracking (limited on iOS)
- Tracks YouTube and Hulu videos (but not videos on other online platforms)
- Location tracking

CONS

- App monitoring doesn't work on iOS
- Advanced web tracking only possible through limited and easily disabled plugin
- Very limited social media supervision
- Doesn't monitor online gaming

PRICING

$49.99/year, unlimited devices

COVENANT EYES

Covenant Eyes has a relational model that encourages accountability, and was specifically created to prevent porn use. It takes periodic screenshots and sends your search history to your "ally" (your accountability partner).

PROS

- Content filtering based on six customizable sensitivity ratings
- Forces safe search across all browsers
- Time limits
- Strong customer support
- Can't uninstall without admin's permission
- Ability to whitelist/blacklist specific sites

CONS

- Easy to find ways around the filter
- Filtering only works when using Covenant Eyes' browser
- Doesn't work for Chromebooks or Kindle Fire

PRICING

Personal $11.99/month, unlimited devices, filtering is an extra $1.50/month
Family $15.99/month, unlimited devices, no extra cost for filtering

Conclusion

Protect Young Minds, a really great anti-porn organization, talks about the importance of teaching kids to develop an "internal filter." We totally agree. Every kid will see porn eventually, even if it's just on their friend's phone at a sleepover. Parents need to prioritize kids' hearts even as they set wise boundaries with the help of internet filters.

We hope this guide helps you figure out which filters would work best for your situation. As you continue in your journey to parent your kids well in our technological world, remember that nothing can replace open and honest conversations with your kids.

As daunting as the Internet and all its content can seem, God is infinitely greater. He loves our kids with reckless abandon. He longs for their hearts to truly love and worship Him, and He's working tirelessly through you and others to make that a reality.

Reflection question

What is your goal for your teen's internet and technology use when they turn 18 (or whenever they leave your house)? How can your current parenting move your teen toward that goal?

Discussion questions for younger kids

- Do you understand why we block certain sites so you can't see them? Do you know what might happen if we didn't?
- What would you do if you saw something online that you didn't understand or that scared you? Would you tell us about it?
- How do you think we'd react if you told us about something you didn't think you should be watching?

Make sure your children know that if they see something inappropriate online, they can and should tell you about it, knowing that you will not be angry but will be thankful they were willing to trust you.

Discussion questions for teens

- Do you think having an Internet filter is a good idea?
- What do you see as the purpose of getting a filter?
- Do you think that the way we've set up the filter gives you accountability without being invasive?
- Do you feel comfortable talking to us if you run across mature content online? Is there anything we can do to help you feel more comfortable?

Related Axis Resources

- *The Culture Translator*, a free weekly email that offers biblical insight on all things teen-related
- A Parent's Guide to Smartphones (covers a "theology of smartphones" and how to decide when to get a child a smartphone)
- 30 Day Smartphone Family Reboot
- Smartphone Sanity by David Eaton and Jeremiah Callihan
- A Parent's Guide to iOS (details how to set up parental controls)
- A Parent's Guide to Android (details how to set up parental controls)
- A Parent's Guide to Pornography
- Porn Conversation Kit (a video series to watch with your teen)
- Check out axis.org for even more resources!
- Join Axis to receive all our digital resources and start a new conversation today!

Additional Resources

- Canopy (use the discount code "Axis" for 30 days free and 15% off forever)
- Qustodio
- Circle
- Kaspersky Safe Kids
- Norton Family
- Covenant Eyes
- "Bypassing content filters: How to see the web they don't want you to see," PC World
- "5 Myths and Truths About Kids' Internet Safety," Common Sense Media
- "What are some good rules for screen names and passwords?" Common Sense Media
- "How can I make sure my kid isn't sharing too much on Facebook or Instagram?" Common Sense Media
- "Google Family Link (for Android)," PC Mag
- "ESET Parental Control (for Android)," PC Mag
- "How to Use Apple's Screen Time on iPhone or iPad," Lance Whitney
- "How to use parental controls on your child's iPhone, iPad, and iPod touch," Apple Support
- "Set up parental controls," Apple Support

Support Axis to get more resources like this!

Thanks so much for reading this Parent Guide from Axis! As a 501(c)(3) nonprofit ministry, Axis invests all proceeds from your purchases back into the creation of more quality content like this. By purchasing content from Axis, you support our ministry, allowing us to come alongside you in your parenting and/or discipleship journey.