



DIGITAL PARENTING FOR DEVICES

Selecting the best one for your child,
preparing them to use it wisely, talking
about parental controls, and creating
a Family Technology Agreement



TECHNOLOGY IN THE PALM OF THEIR HANDS



You know your child has been looking forward to this moment for a long time — **but it still feels like a big step**. Some of your child's friends have one and even share them from time to time. They've been begging for a while, having seen other kids with the latest models, and they're itching to get their very own.

This rite of passage for GenZ is one that didn't exist when parents of today were children themselves: receiving your very own smartphone, tablet, or computer.

As you trailblaze through this uncharted world of digital parenting, you may find yourself feeling unprepared for this moment.

"How did he grow up so fast?"

"Do kids her age need their own device?"

"What kind of device is best for my kid?"

"Will I be able to monitor what she sees on the Internet?"

"How do I use parental controls without snooping?"

"Where's the balance between his independence and safety?"

Whatever your feelings are around this moment — excitement, intimidation, or indifference — we know that **with the right tools and by having a few important conversations, you can give your family all the good of the online world without the bad.**

COMMUNICATION

CONSIDERATIONS THINGS TO THINK ABOUT WHEN SELECTING A DEVICE

What device is best for my child?

You know your child better than anyone. They have unique skills, needs, hobbies, learning styles, and preferences. You're going to select a smartphone, tablet, or computer with features and settings that are just as unique as they are. But which device is right for them?

While there's no one-size-fits-all approach to choosing a device for your child, here are a few questions to consider as you explore and, ultimately, make your purchase:

What's my main motivation to purchase a device for my child?

Is this purchase born out of **necessity or desire**? Understanding this simple but important distinction will help you determine the ideal features, functions, and price point with which you're comfortable. **The first step in this digital device guide for parents is deciding if it's the right time for a device.**

Make a simple list to compare wants versus needs to help determine if your child is ready for the responsibility of a device.

For example, they *need* to call you for a ride after practice, but they *want* to download apps to communicate with friends on social media and play endless video games. Could a phone or watch with calling and texting capabilities give your child the ability to communicate with you without Internet access or unlimited data?

Remember that no matter why you choose to purchase a device for your child, it brings with it some challenges in digital parenting.

How will the device be used?

Consider **key functions** such as calling, texting, Internet access, camera, and storage (documents, photos, videos, music, e-books, etc.). Will your child be using this device for academics or for other reasons? A salesperson may be eager to sell you the latest model with unlimited data, talk, and text or the newest, best, biggest everything, but you may find that a digital device with simpler features better suits your budget and your child's needs.

Will your family purchase a new device every year or two? Or do you expect your child to use this particular device for many years? Does your plan provide any kind of upgrades after an allotted amount of time? Your child's needs will change as they mature, and you'd like to get a device that grows with them if they will be using it for more than a couple of years. Research what features can be upgraded, activated, or added later.

Don't overlook the value of phone insurance. Think of it this way: *None of us were likely responsible for something in our pocket that cost more than \$1,000 when we were kids!* While you want and appropriately expect your child to be responsible, insurance may be a useful investment.

Where will the device be used?

Do you want your child to use apps to help with academics while you work from home? Will your tween be allowed to watch movies on long car trips? Does your teenager need to call you from the baseball field when the game ends?

Thinking about your child's device in terms of location will also help you narrow down the best fit. Airplane mode, Bluetooth pairing, Wi-Fi, and a range of other features can be customized.

YOUR NEXT STEPS

Decide

Does your child truly need a device right now? Get honest. It's OK if the answer is no!

Determine

What features does your child need? Think about. . .

- **Engagement** || *How they'll communicate*
- **Education** || *Tools they'll need for school*
- **Entertainment** || *Features just for fun*

Discuss

Do you want to purchase a device that meets your kid's needs today and can be replaced later or one to last for several years? What will an average day of use look like?

Deciding on the Right Device

As you answer these questions, you'll identify priorities to use to select a device.

Your Child. . .	Device Features to Consider
. . .loves photography, making videos, and creating graphics.	Camera, storage, the ability to download apps
. . .enjoys gaming and digital streaming.	High RAM, graphic quality, the ability to download apps
. . .needs to contact you after school or stay in touch with family.	Limited features outside of calling or texting
. . .is always on the go.	Battery life
. . .will use the device for school and homework.	Word processing, spreadsheet and presentation software and a web camera (this is particularly helpful if your child is doing online school due to the pandemic)
. . .will likely use the device for only a year or two.	The features and functions you will allow your child to use today with no concern for the features and functions you will allow them to use as they get older
. . .will be expected to use the device for several years.	Longevity, updates, and turning off some features now that could be activated at a later date
. . .is a social butterfly and wants to communicate with friends through video chat.	Camera, the ability to download apps
. . .is an avid reader.	E-reader capabilities, storage



CONVERSATIONS DIGITAL TOPICS EVERY PARENT SHOULD ADDRESS

What Should We Discuss

Long before a purchase is made, you can begin talking with your child about the responsibilities associated with owning a smartphone, tablet, or computer. Initiate two-way conversations — not lectures — to encourage **a healthy, open dialogue in your home about technology.**

Think about how you approach conversations about topics such as safe driving, alcohol, drugs, and sexuality with your kids. You want them to take these topics seriously and know they can trust you, come to you with questions, and feel safe in the conversation. The same goes for technology conversations.

Technology is amazing, and when the right steps are taken, it's a wonderful tool that can educate, connect, and inspire.

At the same time, when technology is misused or abused, consequences can be damaging, life-altering, and have negative ripple effects.

As opportunities arise to discuss technology with your child, think about incorporating the following topics:

Digital Citizenship

The concept of “digital citizenship” can help children understand the similarities between navigating a physical community or neighborhood and navigating the digital world. In the same way that citizens of a town do their part to keep the environment clean, safe, and enjoyable for all, a “digital citizen” must do the same.

Google has created a [Be Internet Awesome](#) guide for parents to use with their children to teach them "the fundamentals of digital citizenship and safety so they can explore the online world with confidence." There are games your child can play and a curriculum you can use to teach them to be a responsible digital citizen.

Digital Media

When it comes to digital media — photos, videos, messages, and audio — initiate conversations with your child about what is appropriate to view, send, and receive. Rather than dictate terms and criteria, you can gain tremendous insight into your child’s world by inviting them to share their thoughts first.

Use simple prompts:

- 1. What do you think is appropriate to view or send others?*
- 2. What should you do if someone sends you or asks you for something inappropriate?*

Upon hearing their response to these questions, you can offer additional guidance and encouragement that builds their sense of confidence, not confusion, around the topic. Plus, you’re showing your child that you trust them enough to ask their perspective.

“

Technology is amazing, and with the right tools and information, you can give your family all the good of the online world without the bad.

Digital Footprint

Beyond discussing what kind of content is proper to view, send, and receive, help your child understand the concept of their “digital footprint.” Like a footprint in concrete, emphasize the permanent nature of sharing anything electronically and how it can have lasting effects on reputation, character, and livelihood.

Debunk the popular myth that content shared on a “private account” is safe and secure. The ability to screenshot, save, edit, and repost anything allows other users to transform nearly any so-called private content into the public domain, so **encourage your child to use discretion**. Remind your child that material sent to just one person can be found by anyone.

It’s also critical to understand ownership of content. Social and digital media companies own all content (including messages) on their platform, making it nearly impossible for users to have any true sense of privacy online.

Like a footprint in concrete, emphasize the permanent nature of sharing anything electronically and how it can have lasting effects on reputation, character, and livelihood.



Digital Manners

Have a discussion with your child on the importance of **showing respect to themselves and others** when engaging online. When interacting with others strictly through screens, a sense of anonymity can overpower a sense of dignity.

When we're connecting face-to-face, body language and expressions give us clues, but many of those clues aren't available through a screen. You can't see faces, hear tone of voice, or notice when someone starts shifting their feet because they are uncomfortable. Talk with them about what it looks like to be just as kind online as they are in person.

Words, images, behaviors, and attitudes that a child would never display in person can manifest online in the form of a "dual personality" or fake profile. Explain how this duality is unhealthy and unfair to everyone involved, and the best policy is to be authentic, both in-person and online. Ultimately, this leads to healthy relationships in real life.



Digital Security

In the same way that physical keys provide security to a house, car, or personal property, help your child recognize the importance of **safeguarding the “keys” to their digital property** and their devices. As they’ve likely never been the victim of identity theft, hacking, or cyberattacks, you may have to use analogies and personal stories to explain the gravity of this.

Password management is another important discussion point. For many families, a password management system, like [1Password](#), is a helpful tool. It’s convenient. No more headaches trying to remember what password belongs with which account.

Many of these systems have security protocols in place, so your child’s accounts will be less vulnerable to password-based attacks.

As a family, discuss best practices to keep your digital information safe. Key talking points may include:

- Create memorable passwords without using personal information, such as names, birth dates, addresses, phone numbers, or a family member’s maiden name (a common security question).
- Frequently update passwords, using a mix of uppercase, lowercase, symbols, and numbers to create variation.
- Share usernames and passwords with parents and with parents only.
- Store usernames and passwords in a secure place and never share them in the same piece of electronic communication, such as an email or text message.
- Regularly log out of devices and accounts, especially on shared or public devices and networks.
- Do not use the same password for multiple accounts or devices.
- Be cautious about allowing browsers or accounts to save passwords.

Digital Downloads and App Accessibility

Think through whether or not your child will be allowed to independently download apps, games, upgrades, and software updates. If they are allowed, familiarize yourself with the various content ratings provided by tech companies so you can determine **what level is appropriate for your child**.

[Amazon](#), [Google Play](#), and [Apple's App Store](#) have different rating systems, so age-appropriate content may vary from platform to platform. The use of a parenting review website, such as [Common Sense Media](#), may offer additional insight.

Customize parental controls for greater oversight on in-app purchases, purchases requiring a password, and automatic downloads. Remember, with **purchasing power comes an additional layer of responsibility and accountability** that your child may or may not be ready to handle, so approach this topic with discernment.

It's also important to note that some free apps (specifically games) allow users to make "in-app purchases," such as adding tools to solve a puzzle or to get to the next level. Once an app is downloaded from an app store, there isn't always clear communication within the app that the "extras" will cost money, and any unintentional purchases will be charged to the credit card on the account (even if your child is not able to download new apps). Before allowing your child to download an app, especially a game, it's important to research if it includes these hidden costs and set up clear guidelines for how your child will use it.

You can learn more on our blog about [Apple parental controls](#) and [Android parental controls](#).



Above all, the most effective way parents can help their children succeed in the digital era is to keep communication open and honest.

Digital Expectations

Once you've had an open, honest conversation with your child about the best practices and family policies on device and Internet usage, **it can be a good idea to create a "Technology Agreement" to memorialize what you've discussed** and keep all parties accountable.

You can use our Family Technology Agreement at the end of this e-book or reference it as inspiration to create your own. Approach it as a family project with each member offering input for the suggested guidelines and consequences.

While a document like this can be perceived as restrictive to your child, talk about how it actually helps them avoid getting in trouble and surprise consequences. Conflict often arises when unspoken expectations are not met. An agreement like this ensures that everyone understands what's expected and what the consequences will be in advance.

Parents, please note that if you agree to specific consequences, it's important to stick to those when the time comes, no matter how harsh, inconvenient, or soft they may feel.

YOUR NEXT STEPS

Decide:

- What guidelines do I need to establish for sharing content, saving passwords, app downloads, and private accounts?
- What does it look like, feel like, and sound like for my child to use devices appropriately?
- What does my child need from me most to be successful with this device?

Determine:

What kinds of activities will I allow my child to do on their device?

- Sending and photos and videos
- Downloading free or paid apps, music, videos, and games
- Connecting with friends through social media or messaging apps
- Handling sensitive information like passwords and personal information

Discuss:

- What kinds of downloads are appropriate, and which ones are off-limits?
- What social media connections will you or won't you allow?
- What steps should you take to protect your identity?

CHALLENGES

2

CURRENT ISSUES

DIGITAL CHALLENGES EVERY PARENT SHOULD ACKNOWLEDGE



Digital Parenting

It goes without saying that a driver's permit and a set of car keys don't mean a teenager knows everything there is to know about driving. Your child needs to learn the rules of the road, including speed limits, stop lights, and street signs. They need to take cautions to stay safe in their car, too, such as wearing seat belts and not touching their phone while behind the wheel. And then there are the other challenges that come with driving that aren't about the act of driving, such as questions surrounding curfew and where they are allowed to drive.

In the same way, receiving a new device doesn't mean your kid is equipped with the discernment, maturity, and skill set to use the device responsibly. Remember, as a child, you didn't have access to everything ever put on the Internet and seemingly endless apps and systems to communicate with strangers around the world in the palm of your hand (smartphones only became popular with the release of the iPhone in 2007). You have the opportunity to guide your child in how to interact with technology wisely and set an example for them by the way you use your devices.

While open communication and clear guidelines can help prepare your child to have a healthy relationship with technology, the ever-changing nature of the digital world requires you to **stay informed, engaged, and vigilant to address new challenges as they arise.**

Inappropriate Content

A recent study indicates that 50% of kids ages 11-13 reported having been exposed to pornography. This is also the same age range where many children receive their first smartphone or tablet.

While it could be written off as a coincidence, dozens more statistics reveal a strong correlation between a child's access to technology and their exposure to pornography. Circumstances that prevented or made it difficult for children to view explicit content were eliminated when the smartphone became a must-have item for every member of the household. Unfortunately, this means digital savvy parents must familiarize themselves with where kids might be exposed to pornography and how to prepare them to respond.

Inappropriate content can also come in the form of violence, illegal activity, drugs, language, and other activities you may not want your child to see. Websites and apps that allow user-generated content oftentimes don't come with family-friendly filters. For example, there have been videos of violent crimes posted on Reddit, and there's no warning that they will appear on your screen.

Consider blocking apps and websites like that and also talking with your child about how you hope they will respond if they do see something that is disturbing. While these conversations may be difficult, **you can feel confident knowing you're helping build a solid foundation for a lifetime of using technology wisely.**

To prevent your child from being exposed to pornography, block specific websites, and prevent your kid from accessing certain apps, Canopy works well and has the only [filtering app](#) that can block explicit content in real-time.

YOUR NEXT STEPS

Decide

How should I approach blocking inappropriate content to protect those I love most? What content should I block?

Determine

How and when will I talk with my child about pornography?

Discuss

How do I hope my children will respond if they are unintentionally exposed to inappropriate content?



Contact and Communication with Strangers

Advances in technology now enable individuals to connect with others on the other side of the world within seconds, many of whom they are meeting for the first time. Unlike an in-person introduction, an interaction that happens strictly through digital screens — whether via text, chat, or video — can offer little context on the other person’s intentions, body language, and character. Remember “stranger danger”? **It’s trickier to navigate in the digital world.**

Take heart: Ultimately, it’s unlikely your kid will be contacted by a predator. But with [1 in 25 youth](#) receiving an online sexual solicitation where the solicitor tried to make offline contact, there is a possibility.

To protect your kid, it helps to understand how predators operate. The process is sometimes called “[grooming](#),” and it often seems innocent at first. An adult may take an unusually special interest in a child, buy gifts for them, or connect with excessive flattery. While this may seem harmless initially, this can lead to a dangerous connection with a predator. This is why it’s wise for kids to never accept requests or reply to messages from strangers.

After identifying these red flags, **offer clear action steps** your child should take to handle these situations and to get a parent or trusted adult involved immediately.

Communication from a stranger that your child should tell you about immediately:

- Initiating private conversations or meetings without parental permission
- Acting overly interested and overly eager to connect
- Wanting to exchange personal details such as age, location, or photographs
- Requesting private information like logins, account details, email, password, or phone numbers
- Making an offer that seems “too good to be true” (a gift, winning a contest, money, etc.)
- Using language or imagery that is inappropriate, explicit, or hateful
- Leaving you with a “something just isn’t right” feeling



YOUR NEXT STEPS

Meeting People Online

One reason children and teenagers often want their own device? **Social media**. If they're active on any platform, it's not a question of if a child will meet someone online, it's when. Even narrowing the radius to just your children's known, trusted, and real-life friends poses possible challenges.

Determine what security settings your child should have on their profiles. Are they prepared for the responsibility of receiving friend requests from people they may not know?

Think through all the accounts your child has. Most platforms today have a commenting or messaging component — even exercise trackers or e-book profiles. It's important to understand what communications are possible on what platforms and how to manage privacy settings.

Even if some profile aspects are private, certain information on platforms can still be uncovered. For example, TikTok allows anyone, even if your profile is set on private, to see your username, real name (if provided), and bio. You'll need to dive deep into the privacy tab for each platform to keep your child safe.

Decide

What ground rules will I set for my child to communicate with friends and strangers online?

Determine

What privacy settings are appropriate for my child on different platforms?

Discuss

How will we respond to connections from people we don't know? What are red flags to notice, and what steps will we take to stay safe?

Financial Security

As previously mentioned, if you choose to give your child the ability to make purchases on their device, remember you are essentially trusting them with access to the credit card connected to their device. Careless purchases and online mistakes can have a life-long impact on your credit, so it's best to offer clear guidelines before — not after — an accident happens.

Identity Theft

Because your child may be fairly new to the concept of a digital footprint and identity, it's worthwhile devoting a little extra time to discuss the serious nature of identity theft. From seemingly harmless activities, like impersonating a friend as a prank, to more serious offenses, like obtaining passwords and personal information, **identity theft can come in many different forms.**

More than [one million children](#) were victims of identity theft in 2017, and children are [51% more likely](#) than adults to have their identity stolen, so this conversation is a worthwhile one. Err on the side of caution by ensuring they understand what identity theft is, how people do it, and why it can pose a serious danger to not only them but also those they love.

Specific points to cover on this topic may involve:

- **When and where to access financial accounts (for example, not over public Wi-Fi)**
- **Approved methods for sending and receiving money (apps like Venmo, PayPal, or Apple Pay, etc.)**
- **Guidelines for if or when it's appropriate to share social security information, driver's license numbers, addresses, birth dates, or phone numbers**
- **Purchasing threshold and which items require advanced parental approval, including in-app purchases**

Hackers and Spam

Building on the concept of identity theft, **encourage your child to use discretion** when clicking on emails, links, images, and messages from unknown sources. While some online predators are seeking information for personal or financial gain, many hackers and spammers are simply seeking to wreak havoc. A hacker could permanently disable your child's precious, new smartphone, tablet, or computer.

Bottom line: Make sure your child knows to never click a link or reply to a text from someone they don't know, or if someone offers them something, like a prize, even from a familiar company like Amazon. Those links are not often actually from where they say they are from.

YOUR NEXT STEPS

Decide

What (if any) purchasing permissions will I give my child on their digital device? Apps, online shopping, music, movies, TV shows, e-books, games, or none of the above?

Determine

How will I hold my child accountable for keeping financial and personal details private?

Discuss

How do we identify suspicious links or requests? What are our family's ground rules for how to respond when we receive unknown requests?

Tech Addiction

We often think of technology addiction as something that only affects the workaholics among us, but this is no longer an adults-only challenge. A 2019 census reported that teenagers are now clocking as many as seven hours

per day of screen time, and that's not including time spent on devices for school or homework or during the 2020 pandemic.



The challenge even extends to bedtime, with 72% of preteens and 82% of teenagers saying they sleep with their phone next to them. That's why **boundaries and physical limitations** on where devices are used can help, especially if established when a child first receives one.

Technology offers such a high level of convenience, instant gratification, and access to infinite knowledge, it's a slippery slope to addiction. For this reason, it's critical for families to discuss the realities of tech addiction and make a plan to keep the entire family accountable.

“

Technology offers such a high level of convenience, instant gratification, and access to infinite knowledge.

Beyond the unhealthy consequences presented by any kind of addiction, consider how incessant use of technology could be undermining your values and goals as a family.

Use any of these prompts to begin the dialogue with your family:

- Who do we want to be as a family?
- What are our goals, values, and priorities as a family?
- How does technology move us closer to or further away from those goals?
- Are we using technology mindlessly or mindfully?
- Is technology distracting us from important things that need our attention?
- How can we use technology to bring us closer together as a family?
- What tangible steps will we take to make sure technology doesn't overwhelm our lives?
- Where are our family's "off-limits" times and places for technology, like during dinner or in bedrooms?

Approaching the subject of tech addiction with intentionality and transparency will send a clear message to your child that quality time — not screen time — is your primary concern. **Technology should serve families first, not the other way around.**



Social Media

Similar to the way the smartphone has forever transformed communication styles, habits, and preferences, social media has **irreversibly changed how individuals socialize, conduct business, consume news, and entertain themselves.**

The ability to broadcast any piece of content to a worldwide audience with the press of a button used to be a privilege given to only journalists and reporters.

To help your child understand, here's an analogy: your 11-year-old is given the microphone to anchor the evening news. It's hard to imagine they would be ready to handle that kind of responsibility without any kind of training or preparation.

But that's exactly what social media has done. With only a profile, social media offers that capability freely to everyone with access to the Internet. And to take the analogy further, your kid decides to share more than just the headlines: the latest middle school gossip and friend drama, personal contact information, private details about your family, photos of them and their friends. . .the list goes on and on. And often, our kids just don't have the maturity levels necessary to discern what's smart to share and what's not without being taught.

Each platform should offer a safety center where you can adjust the settings and parental controls to suit your preferences.

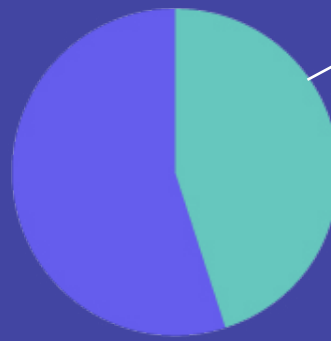
As your child begins to express interest in social media, consider incorporating these key topics into your discussion:

- **Does your child need to notify you before opening a new account?**
- **What are the parameters on private versus public accounts?**
- **How will usernames and passwords be shared with you?**
- **What kind of content is appropriate for the specific platform?**
- **How much time per day can be spent on the specific platform?**
- **How can comparison, cyberbullying, and peer pressure sour the experience?**
- **What action steps can we take together now, as a family, to ensure we stay emotionally healthy while using social media?**
- **What action should your child take when questionable situations arise?**
- **What consequences are there if agreed-upon guidelines are not honored?**

Then there's the potential impact of social media on a child's self-esteem. 45% of teenagers say they feel overwhelmed by all the drama on social media. Roughly four in 10 report feeling pressure to only post content that makes them look good or will result in likes. And 26% say social media makes them feel worse about their own life.

Parents must treat social media as a powerful tool that their child must be prepared to handle maturely and responsibly. Familiarize yourself with the popular social media platforms your child may want to join.

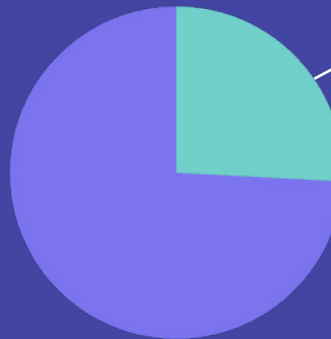
It can be helpful to remind your child how social media impacts their "digital footprint." **Your intention with these conversations is not to micromanage them, but rather it's to set them up for success.**



45% of teenagers say they feel overwhelmed by all the drama on social media.



40% of teenagers report feeling pressure to only post content that makes them look good or will result in likes.



26% of teenagers say social media sites make them feel worse about their own life.

YOUR NEXT STEPS

Decide

What time frame will your child be allowed to use their digital device? What parental controls will you put in place?

Determine

How will your child be allowed to engage on social media?

Discuss

When is it time to reassess social media guidelines?



Cyberbullying

59% of teenagers report having experienced cyberbullying, and Instagram is the platform where this happens most often. Cyberbullying doesn't have to be within a social media app. It's easy for a joke in a text thread to quickly deteriorate to trashing someone who is or isn't part of it. **Words are powerful, and once they are spoken or typed, they can't be taken back.** The way a child talks to or about another person can have defining effects in childhood and adolescence. Prepare your child to identify cyberbullying and how you hope they will respond, even if it might, at first glance, seem like "just joking around." You might also consider a conversation about how they can respond and should come to you if they are the victims of cyberbullying via digital comments, pictures, or messages.

Respecting Boundaries

Different families have different rules for technology, posting photos, and sharing information electronically. Remind your child that **before ever posting or messaging a photo of someone or personal information about someone else to ask their permission.** Also, when your child has a friend take a photo of them, encourage them to ask that friend not to share it digitally if they are not comfortable with it or if you don't allow photos of your child to be online.

Suicide, Self-Harm, and Abuse

The anonymity of the online world (or seemingly anonymous feeling) can lead to some kids sharing things they wouldn't typically share in person: suicidal thoughts, stories of abuse by others, and self-harm.

As your child begins to communicate digitally, remind them that they may hear stories from other kids (anyone under age 18) and should tell a trusted adult *immediately*. **Breaking a promise to "keep a secret" could save a life.**

Drugs, Violence, and Illegal Activities

Access to the Internet is a gateway to endless news stories, how-to guides, videos, and other content about drugs, violence, and illegal activity.

Whether your child sees images or reads a message from a friend, comes across a news story, or stumbles upon dangerous content in an online search, encourage them to talk to you about it immediately. **They may not know how to process what they have seen or could even help someone who is in trouble.**

YOUR NEXT STEPS

Decide

What do I want my child to be prepared to read and see online and when communicating digitally with others?

Determine

How will we keep the conversation open to talk about the following:

- Cyberbullying
- Respecting boundaries
- Suicide, self-harm, and abuse
- Drugs, violence, and illegal activity

Discuss

- What is cyberbullying, and how can you respond to it?
- How do you handle information about and photos of others?
- What should you do if someone is talking about suicide, self-harm, or abuse?
- What kinds of content about drugs, violence, and illegal activity should you discuss with a parent?

CONTROLS

3

PARENTAL CONTROLS PROTECT THOSE YOU LOVE MOST

Digital Parenting

We'll let you in on a little secret: We don't like the phrase "parental controls." We use it because that is what parents search for online, but we look forward to the day when the phrase "digital parenting" can replace it. Because that's what this is actually about. You are trying to parent in the digital world, just like you would in the real one. Most parents don't dream of their kids calling them "controlling," and most kids cringe at the thought of being "controlled."



Parenting does, however, require setting up healthy boundaries, which isn't always easy, and we want to support and applaud you for all that you do to encourage healthy habits and protect your child. You feed them nutritious food when they are young with hopes that they'll make healthy choices when they are adults. You have them wear a bike helmet and a seatbelt.

Those guardrails don't prevent them from ever making an unhealthy choice or getting hurt, but if they were to stumble or get in an accident, they will be better protected.

Protecting them online with parental controls is important, too, and it's hard and different than parenting in a world without the Internet in the palm of everyone's hand.

Technology is Part of the Solution

The question remains: How do you, as a parent, encourage your child to leverage technology, because it's amazing, while also keeping them safe with parental controls? The good news is that [adding parental control apps to your family's life can be done in a way that honors both your child's growing autonomy and your responsibility as a parent to keep them safe online.](#)

Settings on specific devices, operating systems, and platforms can offer you some additional oversight without eroding your child's sense of independence and privacy. Take time to become familiar with the parental controls, privacy settings, safety centers of all the systems and apps to which your child has access. Here are some of the ones that you may use:

Social Media and Communication Apps

- [Snapchat Privacy Settings](#)
- [Facebook Safety Center](#)
- [Instagram Safety Center](#)
- [Twitter Safety Center](#)
- [TikTok Safety Center](#)
- [YouTube Parental Controls](#)
- [WhatsApp Privacy Settings](#)
- [Discord Safety Center](#)
- [Messenger Kids Parental Controls](#)

Search Engines

- [Google Safety Center](#)
- [Bing Safety Center](#)

Device and Operating Systems

- [iOS Parental Controls](#)
- [Android Parental Controls](#)
- [Microsoft Safety Center](#)

Streaming Systems

- [HBOMAX Parental Controls](#)
- [Hulu Parental Controls](#)
- [Sling Parental Controls](#)
- [Peacock Parental Controls](#)
- [Netflix Parental Controls](#)
- [Amazon Prime Video Parental Controls](#)

Canopy Protects Those You Love Most

Canopy's software is the culmination of years of research and development guided by experts in technology, medicine, and public health. We envision a world in which search engines, marketers, and anonymous strangers can't dictate what your child sees online.

Our team has devoted the past ten years to developing world-class, patented technology that is as dynamic as the modern Internet. At a high level, **Canopy gives your family all the good of the online world without the bad.**

Leveraging advances in artificial intelligence, machine learning, and real-time scanning, we can deliver a healthy, pornography-free Internet experience.



Real-Time Scanning || Canopy uses patented technology to scan websites in milliseconds, detecting explicit content in real-time. Thanks to this advance, we are not dependent on a potentially out-of-date catalog of bad sites. Our solution prevents exposure.



Sexting Prevention || Canopy has the ability to scan and analyze photos taken by the device's camera and can flag those that might be inappropriate.



App Management || Easily cut off Internet access for specific apps or games while still allowing your child access their device's productive and parent-approved features.



Tamper Proof || Canopy's sophisticated anti-tamper measures prevent the app from being removed or disabled without parent notification.



Location Awareness || Keep up with your kid all day, no matter where life takes them with Canopy's location awareness feature.



TECHNOLOGY AGREEMENT



EXPECTATIONS HOW YOUR FAMILY WILL USE DEVICES

You Know Your Child Best

The following pages have a checklist for you and your child to discuss when, how, and where you will interact with technology. There may be items listed that you choose not to include in your family's agreement, and that's OK! Simply check the ones that apply for your family.

Also, as your child gets older, you may choose to change what is included in the Technology Agreement. You can update it whenever you feel your child is ready for more responsibility. Our hope is to encourage open and honest conversation about technology.

Set the Example

As you hold your children accountable, consider how you can appropriately do the same. Your children will learn more from watching you than from what you say, and they are watching.

Everyone Participates

Of course, as a parent, there are certain guidelines that are not up for negotiation; you are the parent, and they are the child. However, to inspire willing compliance, complete the following agreement together and talk through the decisions made, depending on what is appropriate for the age and maturity level of your child.

OUR FAMILY TECHNOLOGY AGREEMENT

EXPECTATIONS HOW OUR FAMILY WILL USE DEVICES

Device-Free Activities

- ☐ Meals shared with other people
- ☐ During school or homework time
- ☐ During practice and group activities
- ☐ In the car
- ☐ While someone is speaking with me
- ☐ Practice, rehearsal, or lessons

☐ _____

☐ _____

☐ _____

Device-Free Times

- ☐ In the morning before _____ am
- ☐ In the evening after _____ pm

☐ _____

☐ _____

☐ _____

Device-Free Places

- ☐ School
- ☐ Cars
- ☐ Place of worship (church, synagogue, etc.)
- ☐ Bedrooms
- ☐ The basement, den, or other closed-door rooms in the house
- ☐ Bathrooms

☐ _____

☐ _____

☐ _____

Stored and Charged Location

Device Agreement

- ☐ If my phone breaks, I will tell a parent exactly how it happened, honestly and in a timely manner.

● A parent will have the login information for all of my accounts. I will tell them if I change it.

● A parent can ask to see my device at anytime.

Screen Time Boundaries

Time for school or work

Time for games

Time for social media

Time on the app that is the most distracting

Time to watch movies and TV shows

Personal Information and Security

How we will create and store passwords

Purchases I can make on my device

I will keep private:

- ☐ Full Name
- ☐ Address
- ☐ Phone
- ☐ Credit Card
- ☐ Birth date
- ☐ Email

Content

- I understand what is appropriate content to send and receive.
- I will tell a parent if I receive or am asked for something inappropriate.
- I will tell a parent or trusted adult immediately if someone I know talks about:
 - suicide, self-harm, or abuse.
 - acts of violence, drugs, or illegal activity.
- I will tell a parent or trusted adult immediately if I see or read:
 - cyberbullying.
 - pornography.
 - something that makes me feel uncomfortable or scared.

-

Apps, Games, and Social Media I'm Allowed to Use

- A parent has to set privacy settings.
- I will not make in-app purchases.

Communication

- The requirements for me to accept a message, contact, friend request, follow, etc., from someone (select one):
 - I know them in real life and a parent knows them.
 - I know them in real life.
 -
- I will never click on a link sent by a stranger or company (if I did not request the link or sign up for it).
- I will not electronically communicate something that I would not say face-to-face.
- I will not engage in cyberbullying, including but not limited to group messages, texts, memes, videos, and comments.
- I will ask permission from someone before digitally sharing a photo of or information about them.
- I understand that if I send a photo or text, even in an app where it will disappear quickly, someone could screenshot it and share it with the whole school, on their own social media channels, and on public platforms.
- I will respect others by the way I talk to and about them digitally, whether I know them in real life or not.
- If a stranger offers me a prize or gift, I will not accept it and will tell a parent immediately.
- I will be the same person I am digitally as I am in real life, not making up false information about myself.
- I will only share information online that is appropriate to share with the whole world, not sharing anything personal, identifying, or private.
- I will ask family members before digitally sharing photos of or information about them online.
- If I have questions about my body, sexuality, illegal activity, violent events in the news, pornography, or drugs, I will ask a parent or another adult who I know my parents trust instead of searching online for answers.

-

We Agree

We will revisit this contract on _____ together to see if there are any needed changes or updates.

When a mistake is made, we agree to talk about it honestly and calmly, and the consequence will be:

I agree to approach technology responsibly, respect both myself and others, keep communication with my parent/child open, and take good care of devices and myself. I agree with our family's decisions above, and I agree to be open to questions about technology.

- ***PARENT ONLY: My child will not be punished for asking me a question or telling me about something inappropriate they see online or from a friend.***

CHILD SIGNATURE

PARENT SIGNATURE

ACTION PLAN



CHECKLIST HOW YOU WILL PREPARE YOUR CHILD FOR THEIR FIRST DEVICE

Customize the Conversation

Depending on the age and maturity of your children, you will choose to emphasize different conversations with different levels of importance. To not feel overwhelmed by all the possible topics you could cover to prepare your kid to use a device wisely, work through this checklist first, selecting the ones that you know you need to discuss because you know your kid best. You can always revisit the list and conversation later, especially as your child matures and earns more responsibility and privilege.

PREGAME STRATEGY

- ☐ How my child will use this device
- ☐ What device is best for them

PRACTICE

- ☐ Digital citizenship
- ☐ Digital media
- ☐ Digital footprint
- ☐ Digital manners
- ☐ Digital security
- ☐ Digital downloads and app accessibility
- ☐ Digital expectations

GAME TIME

- ☐ Inappropriate Content
- ☐ Contact and communication with strangers
- ☐ Meeting people online
- ☐ Financial security
- ☐ Identity theft
- ☐ Hackers and spam

- ☐ Tech addiction
- ☐ Social media
- ☐ Cyberbullying
- ☐ Respecting boundaries
- ☐ Drugs, violence, and illegal activities

THE REFEREE

- ☐ [Parental controls conversation](#)
- ☐ Set up parental controls
 - ☐ Operating Systems
 - ☐ Devices
 - ☐ Games
 - ☐ Apps
 - ☐ Social media platforms
 - ☐ Streaming services
 - ☐ Search engines
- ☐ Add [Canopy](#), the only real-time porn blocker that also deters sexting
- ☐ Complete a Family Technology Agreement