CANOPY

DIGITAL PARENTING

Guiding your child to be a wise digital citizen, understanding digital parenting tools, and creating a Family Technology Agreement

Version 2.0

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 devices 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**.

WHICH DEVICE?

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
. . .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

DIGITAL CITIZENSHIP

2

COMMUNICATION
WISE DIGITAL CITIZENSHIP IN A COMPLEX DIGITAL WORLD

Digital Citizenship

Being a wise digital citizen is not something kids (or we!) are born with or wake up knowing. Children and teens may be the most tech-savvy creatures on the planet, but they are (sometimes) also the most unaware about how to be wise digital citizens.

The concept of "digital citizenship" can help them (and us!) 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" does the same online.

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 and a curriculum you can use to teach them to be a responsible digital citizen.

Long before your child has their own device, you can talk 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.

Consider discussing the following truths about the digital world as you guide your child to be a wise digital citizen.

Digital Citizens Live in Public

There is no private message or disappearing photo that can't be made public. Screenshots, using one device to take a photo of another device, and a quick "copy and paste" are a few of the ways that images and words shared electronically can be saved and shared by the recipient to an unintended recipient.

This is a difficult truth for kids to grasp for two reasons. First, they trust their friends. They believe that the person with whom they are communicating would never share something that wasn't supposed to be shared. Most kids on most days wouldn't, but as preteens and teens navigate the world of adolescents, they sometimes forget to consider the consequences of their actions and make unkind choices.

Talking about this with your children is important and also tricky. The idea of accusing a friend of doing something "bad" will likely not be received well. Instead, talk about how accidents happen. Perhaps you once shared something that you didn't know was meant to be confidential and had a friend be hurt or mad at you? The concept that this could happen is more important to discuss than how and why it could happen. **When kids understand that everything is potentially public, they will be more cautious about what they digitally share.**

Secondly, they trust devices and systems. One idea to help kids understand that information shared on a platform may be owned by the platform is to **have them read the privacy policies** before being allowed to use the platform. Read it with them, and discuss what is actually private and what is actually owned by the company. When they realize what those policies say, they may think twice before hitting send.

> **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.**

When You Share Something as a Digital Citizen, It Doesn't Disappear

Similar but different to the "digital is public" truth, digital is forever. Like a footprint in concrete, they emphasize the permanent nature of sharing anything electronically and how it can have lasting effects.

Only a few short decades ago, when a note was passed between students in school or a photograph shared, it could be torn up into tiny pieces, doused with water, and thrown in the trash, even burned or put through a shredder. It would take a CIA-level forensics lab to even attempt to reassemble the message if there were any physical paper or part of the photograph remaining. Kids could truly destroy something they wrote or a photo of themselves.

All the same ways of saving things that were mentioned above apply here. That not only means that words and images can be shared but also that they can be stored. Forever. It's not entirely unheard of for a business or educational institute to learn more about an individual through social media or an Internet search.

Preteens and teens struggle with the idea of long-term consequences by the very nature of their maturity. Have

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

your kids ask themselves, before posting: "What would I think about it if an adult I admired posted or shared the same thing? Would it be bad?" **One day, they will be grown-ups with authority and influence, and understanding that everyone could potentially bring up their past could be reason enough to make better digital choices.**

Take a few minutes and research public figures and celebrities who have "fallen" because of their past. Everyone makes mistakes, and it's unfair to judge someone as a 50-something for a sentence they said as a 15-year-old. Nonetheless, the world isn't fair, and kids should understand that their posts, comments, and images shared digitally will remain open to criticism forever and could cause them problems years later.

Digital Citizens Can Share Too Much

Full names. Emails. Phone numbers. Addresses. Birth dates. The amount of data systems and strangers can get from profiles is disturbing. The same is true for using public wifi and clicking on links from unknown senders. Hackers don't limit their attacks to adults, and if they can get a child's data, they can make their life miserable as they grow up and begin interacting as an adult.

Referencing the "digital is public" point, **have family ground rules for what is shared in a profile, especially those that are public on platforms or in systems by default**. Read the fine print to know what you can hide from strangers when you are entering personal information. Talk about how to create unique passwords, where to store those passwords, and how never to click on a link sent by someone you don't know. Have expectations for what kind of apps you use to transfer money, and make sure that kids know to never share things like their social security number.

Password management is another important discussion point. For many families, a password management system, like **1Password**, is a helpful tool. No more headaches trying to remember what password belongs with which account.

Digital Citizens are Humans

It is approximately one billion times easier to say something mean across cyberspace than to someone's face. Looking someone in the eye is powerful. Extreme emotions are easier to express when you don't have to look the person in the eye and deal with the consequences. Cyberbullying is outrageously common, especially for young girls.

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.

For example, it may be hard to physically get up and move everyone at a lunch table, leaving one person to eat alone, but it takes less than a second to delete someone from a group chat or post a nasty comment on someone's Instagram post.

Ask your kids to think of a time when someone said or did something hurtful? Then ask them about something hurtful said or done online. They may shy away from sharing a story where they were personally attacked, but they will have plenty of kids being mean, especially digital ones.

Regularly **ask your kids how they see others being kind online**, as well. Together, brainstorm ways to lift up and encourage others proactively. Remind them that those stories matter, and it's not always talking about the hard stuff. A wise filter: "Would I say or do this if I were looking at the person face-to-face?" If not, then don't say or do it digitally, either.

Digital Citizens Can Be Influenced by the Digital World

Words, images, and videos all shape us. Studies show how [viewing porn can be addictive and alter brain chemistry](#), and that is a [massive problem in our world today](#). However, consider how the kind of content your kids consume shapes their behavior in other ways, as well. Most kids (and adults!) will say that media doesn't shape us, but it's difficult not to reflect on what we consume or not become numb to things that should bother us.

One mom of a middle schooler took away the privilege of watching a popular show aimed at preteens because the main character treated her parents disrespectfully. The mom started noticing that after she watched the show, her daughter would treat her and other adults that way. This young preteen had no intentions of being rude or inappropriate. However, she loved this show and thought the main character was "so cool." Even if it wasn't conscious or intentional,

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

she emulated the way the character talked. **Discuss with your kids how media can influence thoughts and behavior, even when it's not intentional.**

Being a Digital Citizen Isn't Always Free or Cheap

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

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.

It's also important to note that some free apps (many 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). Research what downloads include these hidden costs and set up clear guidelines for how your child will use them.

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:
- How have you seen examples of responsible digital citizen?

- When have you seen others be irresponsible digital citizens?

- What is difficult about being a wise digital citizenship, and what do you need to help you make wise choices?

DIGITAL DANGERS

3

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 of 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.

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

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.

YOUR NEXT STEPS

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**.

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**

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.

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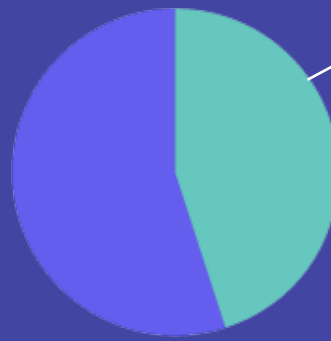
45% of teenagers say they feel overwhelmed by all the drama on social media.

40% of teenagers report feeling pressure to only post content that makes them look good or will result in likes.
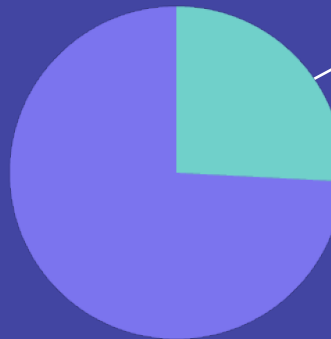
26% of teenagers say social media sites make them feel worse about their own life.

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 or 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**.

Sexting

Most parents know it's important to protect their kids from **sexting**, but most parents aren't quite sure what the conversations should look like, especially with preteens and young teens. It's hard to imagine your child who hasn't completed puberty or started to date needing to understand how to respond if someone asks them for a sext.

Nonetheless, because **two out of every three girls ages 12-18 have been asked for one**, it's a conversation you can't not have. Especially **because 22% of teen girls have sent or posted a nude or semi-nude photo or video of themselves (11% between ages 13-16), and 18% of teen boys have done the same**.

How do you help guide your child to make wise digital choices and avoid sending or posting an image or video they can't take back? Start the dialogue earlier than you think you should, and consider including these conversations in your digital parenting strategy.

Digital is forever and public. Period. End of story. There is truly no foolproof way to ensure something is deleted after it is sent from one device to another, as mentioned previously. Four popular ways images and videos are captured and could be made public or saved permanently:

1. Saving to a device (expected)
2. Screenshotting an image or recording the screen while a video is playing (expected)
3. Using one device to take a photo or video of the screen of another device (not quite as expected)
4. Mirroring what is on the screen of one device to another and then doing one of the three listed above (not quite as expected).

Create opportunities for your kids to learn by allowing them to interact with safe people (like family and family friends) as practice on your devices. Show them the photos you are sending and posting and even talk about a photo you wouldn't post or share and why.

Don't send or post any digital images or videos that you wouldn't want your dad to see. Most kids wouldn't want a picture of them sneezing in the yearbook, but if their dad saw that same picture, it wouldn't make showing up to a family dinner too embarrassing or all that awful. A kid's dad seeing them posing explicitly, in minimal clothing or nude, however, would be horrifying.

Therefore, remind your kid that if it's an image they wouldn't want their dad to see, they shouldn't share or post it digitally.

Don't send or post a digital image or video in an outfit that you wouldn't wear to school. Kids probably wouldn't show up to math class in a bikini, half-dressed, or in underwear, so sending photos clothed (or not clothed) like that is not OK.

Preteens and young teens are still concrete thinkers so having distinct boundaries can be helpful. This is a great filtering question for them to ask before sending an image or video.

Empower them with the freedom to choose. Most girls will feel like they don't have a choice. If they send a photo, they are a slut. If they don't send a photo, they are a prude. Neither feels like a good option. Remind them that the person asking isn't going to flaunt rejection, and if they fail to send a photo, they'll probably leave them alone. It is their choice about how they respond. They are in control of the situation and can decide how to respond.

Give them a script. Have your kids save ideas of how to respond to a sext request somewhere on their device to copy and paste when asked. It's easier to come up with these ahead of time than in the moment. Ask them for ideas, and help them put thoughts into their own words.

It could be child porn. Sexting laws and the penalties for violating the laws vary from state to state. There are multiple factors at play including the age of consent, the difference in age of the sender/receiver, and the specific nature of the image. In some states, teens who are charged with sexting crimes may be required to register as a sex offender.

While a complete exploration of this topic would require an entirely separate discussion, it is important for both those under age 18 and their parents to be fully aware of how **the laws in their state** may impact them when it comes to sexting.

Don't apologize. Remind them that they should never apologize for not complying with a photo request. They will have done nothing wrong, and apologies are for when someone needs forgiveness. The person asking may pressure them and respond as if they are doing something wrong by not sending the photo. That is simply untrue. Not sending a sext when asked for one is not worthy of an apology. Remind your kids, especially your daughters, not to apologize for not sending a sext or any photo they are not comfortable sharing.

PARENTAL CONTROLS

4

PARENTAL CONTROLS PROTECT THOSE YOU LOVE MOST

Keep Your Kids Safer Online

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:

Device and Operating Systems

- **iOS (Apple)**
- **Android**
- **Windows 10**

Social Media and Communication Apps

- **TikTok**
- **Instagram**
- **Snapchat**
- **Discord**

Streaming Systems

- **Amazon Prime Video**
- **Disney Plus**
- **CBS All Access**
- **HBO Max**
- **Peacock**
- **Netflix**
- **Hulu**
- **Apple TV**

How Canopy Uses Filtering to Keep Your Kids Safer Online

Somedays, the choices you make as a parent are easy and fun with little pushback from your kids. They may not argue with you when you tell them they must wear a seatbelt if they are going to drive. It's a normal part of our world and commonly accepted as a precaution to take when in a car. But other choices, such as talking about parental monitoring apps, may be met with more friction.

Fortunately, with Canopy, it's a little easier because we allow you to filter instead of monitoring everything your child does online.

When these apps were first created, monitoring was required. There was no tech that allowed for filtering out explicit content in real-time or in a foolproof way. Parents were simply sent a report of what kids already saw and did on a device...after it happened by parental monitoring apps. Those conversations were hard because most parents probably wished they could have prevented it.

With Canopy's tech, it is possible to filter out explicit content before it has the chance to hit the screen of the device a child is using. It doesn't only block the websites flagged as "adult." Many websites, including popular ones like Twitter and Reddit, allow porn. **It's nearly impossible to not be exposed to porn accidentally if you are regularly online...and don't have Canopy.**

Another challenge with monitoring is that kids, especially teenagers, feel as if their privacy is being violated. Of course, as a parent, you have the right to make sure your child is being responsible and safe online and be as involved in their lives as you feel appropriate!

But there is a way to do that while also giving your child the freedom to explore the digital world and not feel like their parents are "invading their space," even if said space is an illusion and on a device paid for by a parent.

Kids can use the Internet without having someone electronically look over their shoulders because parents know they won't see explicit content. And parents get the peace of mind knowing that those they love the most are safer online with Canopy than without.

You may still want them to have a "digital seatbelt" while they "drive online," but you're willing to hand over the keys to the car, trusting them more and more to navigate wisely. Canopy allows them to do this safely.

How does Canopy do this? 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 to 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

Or 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
- ○ Credit Card
- ○ Address
- ○ Birth date
- ○ Phone
- ○ 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