

A P A R E N T ' S
T O
G U I D E

iOS

axis

“

Every day, every hour, the parents are either passively or actively forming those habits in their children upon which, more than upon anything else, future character and conduct depend.

—Charlotte Mason

iAmOverwhelmed

21st-century parents have to figure out all kinds of digital technology, even if we're not particularly "techie" by nature. It's similar to when we worry about helping a high-schooler with algebra when we ourselves are lousy at math. We can send them to tutors when they grow beyond our experience in math, but digital tech doesn't allow us that same luxury of delegation. It's vitally important that we know (and keep learning) what our teens' devices do, how they work, and how they're being used.

Despite what it may seem like, not everything or everyone on the Internet is out to get our kids, and a few simple strategies implemented via the device's operating system can quickly and regularly protect them from violent content, identity thieves, cyberbullies, porn, and sexual predation. Use these efforts in tandem with relational techniques **aimed at connection instead of control**, and the device becomes a way to strengthen the parent-child bond while still allowing us to prioritize their health and safety.

What does "OS" mean?

It stands for "operating system." Essentially, today's smartphones and tablets are handheld computers. The minute we turn on a smartphone, computer, tablet, video game console, or even a graphing calculator, an OS fires up. The OS runs the device, allows the integration of features and apps, provides the user interface, and keeps the device running smoothly. A mobile OS also connects a smartphone, tablet, or wristwear device to its wireless carrier (Verizon, AT&T, etc.) and to Wi-Fi networks. Current smartphone operating systems include Google's Android, Apple's iOS, Microsoft's Windows Mobile, Nokia's Symbian OS, and Blackberry's RIM.

Not sure which OS is running on a device? The name and version of the device's operating system is available under Settings > General > About (see photo).



What should I know about iOS?

While Android OS is by far the most-used mobile operating system on earth, controlling [more than 80% of the mobile OS market](#), Apple's OS (known as iOS) makes up virtually the rest of the market share. iOS works on about 60 devices and offers [unchallenged compatibility between them](#) (Apple designed all their devices that way intentionally to make iOS users more inclined to only purchase their devices).

All Apple devices come standard with iOS, which has [extended parental controls](#), including the ability to hide certain apps, schedule when the device can be used, regulate who can call or text to and from the device, and notify a parent when the user arrives or leaves a certain location (see below). Also, the iOS [Family Sharing](#) feature allows one adult in the household to oversee shared features on the devices, and up to six family members can share purchases on iTunes, iBooks, and the App Store, as well as a calendar, photo album, and reminders. (It also allows you to find a missing device.)

How do I set up parental controls on an iOS device?

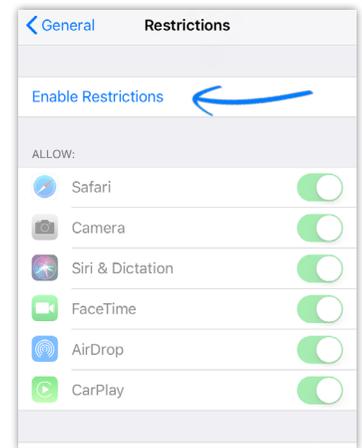
Parents can implement controls (called “Restrictions”) on individual Apple services to help protect their teens and manage usage. Location settings on the device can help a parent find the child when he/she is away from home, or parents can turn the location service completely off to prevent predators from hacking the device and locating the child.



= Settings App

Set up parental controls on an Apple device:

1. Tap **Settings app**, then **General**.
2. Scroll down and tap **Restrictions**, then tap **Enable Restrictions**.
3. Create a Restrictions passcode (Apple advises parents to choose a Restrictions passcode different than the one used to unlock the device). You’ll need this to change settings or turn the restrictions off, if desired.
4. **NOTE:** Keep your Restrictions passcode handy. If you forget your Restrictions passcode, it is necessary to completely erase the device and set it up as a new one in order to remove the old passcode.



Change the Restrictions passcode:

1. Tap **Settings**, then **General**, then **Restrictions**.
2. Enter the current Restrictions passcode.
3. Tap **Disable Restrictions**, then enter the passcode again to confirm you want to disable restrictions momentarily.
4. Tap **Enable Restrictions** and enter a new passcode.

Restrict apps and features:

1. Tap **Settings app**, then **General**, then **Restrictions**.
2. Any app or feature with its slider to the right and showing green is **enabled**  on that device. To disable any app or feature, simply slide to the left . Examples of apps, features, and content that can be restricted:
 - Safari (web browser)
 - The camera (this disables FaceTime)
 - Siri & Dictation
 - AirDrop (sending files via bluetooth)
 - CarPlay
 - iTunes Store (Music, Movies, TV Shows)
 - Music Profiles & Posts
 - iBooks Store (eBooks)
 - Music, Podcasts, News, Movies, TV Shows, Books
 - Specifically rated content
 - Specific websites
 - The ability to purchase and delete apps
 - Gaming (including multiplayer games)
 - The ability to add friends
 - The ability to screen-record
 - Privacy settings, including location, contacts, calendar, photos, Bluetooth, the device’s microphone, speech recognition, advertising, media library, etc.
 - Volume limits, TV provider, cellular data use, and similar settings

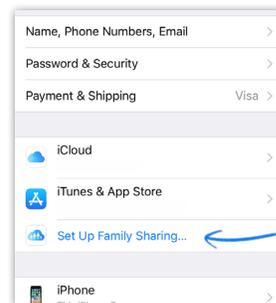
Prevent purchases from the iTunes Store:

1. Tap **Settings app**, then **General**, then **Restrictions**.
2. Enter your **Restrictions passcode** (see above if you haven't set one up yet).
3. Turn off **In-App Purchases**. To disable all purchases on the device, turn off **iTunes Store**, **iBooks Store**, **Installing Apps**, and **In-App Purchases**.
4. Purchases can also be prevented by removing any stored payment methods from the account.

If you prefer to regulate rather than completely disable downloads from the iTunes or App Stores, you can set up iOS to require a passcode for individual downloads.

Enable Family Sharing:

1. Tap **Settings app**, then your name (very top).
2. Tap **Set Up Family Sharing**, then **Get Started**. (On iOS 10.2 or earlier, tap **Settings**, then **iCloud**, then **Set Up Family Sharing**.)
3. Follow the onscreen steps.



Restrict purchases using Family Sharing:

1. Set up **Family Sharing** as instructed above.
2. Tap **Settings app**, then **Family Sharing**.
3. Tap the family member's name.
4. Tap **Ask to Buy**. The Family Sharing organizer (you) will now receive a notification when a family member wishes to make a purchase or download content. You can approve or decline the family member's activity from your device.

To approve/decline a purchase or download request via Family Sharing:

1. Open the notification on the organizer's device.
2. Review the request for purchase or download from the family member.
3. Approve or decline the activity, as instructed (approval will require entry of the organizer's passcode).
4. **NOTE:** Any purchase or download by anyone in the Family Sharing group will be accessible by everyone else in the group. *In addition, if a group member downloads a previous purchase, installs an update, or uses a redemption code, no notification will be sent to the organizer.*



But my kids can get around all of this, right?

Unfortunately, if a teen wishes to get past the controls on their device, the Internet [too easily](#) provides detailed instructions on how to do so. Even if a teen does not personally know how to bypass security settings, most likely their friends can show them how. Some teens make it their business to keep up with new tech and online developments so they can sidestep limitations quickly and at will.

And, if they're desperate, many young people will simply reset their devices to factory settings

to wipe out the limitations placed on it. Although this action clears everything on the device, a user can save the device's information to a Mac computer via a USB cable or a cloud service. Then, after the reset, they simply reload whatever they want back onto the device—minus the parental controls.

[Other methods](#) readily allow savvy teens to hide their internet activity and browser history. These include installing VPN (virtual private network) software, “proxy sites” which divert the device's activity to a different server (similar to using a neighbor's wi-fi), installing a hidden browser on their device, and even using Google Translate as a crude proxy site. But, of course, even if we could prevent our kids from going through all this and have their phones set up with perfect boundaries and controls, they can always just log into their accounts (or create new ones) on a friend's phone later. Or, as a parent recently told us, friends can give their old phones to our kids, which they can then keep hidden from us, and we would be none the wiser.

What do I do if my teen keeps finding ways around parental controls?

If a teen is a repeat offender, we feel your frustration and pain! It can be so grinding to have a child who sees boundaries as simply another challenge to overcome. And while we admire their perseverance and creativity, this desire to subvert authority may point to a deeper issue.

True or false: *The stricter the parent, the sneakier the child.* What do you think? When we ask this of parents at our [live events](#), mothers typically respond that they think it's true, while fathers typically think it's false (there are exceptions, of course). Obviously every child is different, and just because you might be strict doesn't mean all your children will react to you the same way. We think it depends on our view of sin.

If we view sin as something to avoid at all costs, something that shows how terrible a person is and how they've failed, then we will parent our kids that way. If they're caught in sin, we will punish them, tell them how disappointed we are, and tell them we expected better behavior out of them. They may be filled with shame and regret, especially if they still desire to partake in that sin (e.g. just because someone gets caught drinking doesn't mean they didn't enjoy the activity and won't want to do it again). So rather than disappoint mom or dad again, they find ways to continue that behavior without mom or dad finding out. They become **sin-concealers**.

However, if we view sin as a symptom of an underlying issue rather than as the problem itself, we'll take a different approach when dealing with it. When a child is caught deliberately choosing to sin, rather than reacting out of anger and disappointment, we'll take the time to talk to them about *why* they chose that behavior or action, how it affected them, and how it impacted others (in addition to allowing them to experience the consequences of their actions through lost privileges and other punishments). Then we'll also help them see how choosing that sin is actually choosing to settle for less than God's best for their lives, even though it may *seem* on the surface to be satisfying. By having these conversations with them, we help them view sin for the life-stealing, negative thing it is, as well as help them desire what God desires for them. In so doing, they will learn to be **sin-confessors**, i.e. children of God who “hate what is evil,” no matter what enticing form it takes, and who “cling to what is good” ([Rom. 12:9](#)). So much of the journey toward spiritual maturity is dying to the old self and taking on our new creation in Christ.

When it comes to smartphones and the boundaries we put in place for our kids, we need to help them see them for what they are: **boundaries that protect them and keep bad things out.**

Too often we've spoken to teens who felt that their parents only put limits on their phone use because their parents hate fun, are cruel, or are scared of smartphones (or maybe all three). But we've also spoken to many parents who are desperate to help their teens find true, fulfilling community or to keep them from being bullied or to find lasting joy. So there's a disconnect. The only way to bridge the gap is to talk our kids about *why* we do what we do and to allow them to talk to us about how our imposed boundaries make them feel.

G.K. Chesterton [wrote](#), "The more I considered Christianity, the more I found that while it had established a rule and order, the chief aim of of that order was to give room for good things to run wild." Think of ways to help your rebellious teen see boundaries from that perspective. Instead of seeing limits as punishment, help them realize that boundaries are designed to keep them safe. You give them boundaries not because you don't trust them, but because you love them and want what's best for their lives. And never forget that, as powerful as smartphones are, they are no match for the power of our God as His spirit prompts, teaches, admonishes, and leads them in navigating this challenging technology.

Finally, we must remind our teens that while we parents are paying for the phones and they're living under our roofs, *they* don't own the devices; we do. So if they continue to abuse their phone privileges, then we will continue to revoke those privileges until they can regain trust and prove that they're trustworthy. As with any tool or technology we have access to, our use of smartphones is a privilege, not a right.

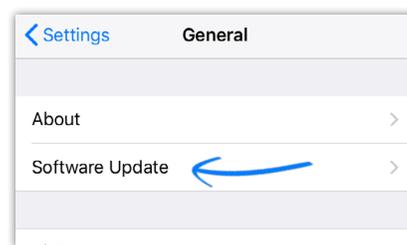
How can I make the most of out of iOS?

Keep the device reasonably updated. Take advantage of emerging technology and stay alert to the newest hazards by installing regular updates to the iOS on the teen's device. Most casual tech users feel tempted at some point to leave an older version on their device, thinking it might be more difficult than it's worth to update and learn the new one. Maintaining effective security measures on the device is the most compelling reason to keep it updated. Older versions will eventually lose access to tech support, won't download newer apps, and more easily fall prey to online threats and identity thieves.

iOS offers regular notifications of available updates. When these notices appear on the device, simply agree to install them as instructed in the notification. These can also be installed manually.

Manually install an iOS update:

1. Connect the device to the Internet via Wi-Fi.
2. Tap the **Settings app**, then **General**, then **Software Update**.
3. Tap **Download and Install**. A message may appear requesting to remove apps temporarily to allow more space on the device for the update; choose **Continue** or **Cancel**. Any apps removed during the update process will be reinstalled once complete.
4. Tap **Install** to activate the installation immediately, or tap **Later** and choose when the update should install automatically.
5. Enter your **passcode** as requested (the passcode used to unlock the device, not the restrictions passcode).



Learn how to navigate an iOS device. iOS uses a screen called “Control Center” to organize the device’s common settings and features (see photo). To access it, swipe up from the bottom of the screen, then simply tap the appropriate button or slider to adjust the setting. When finished, swipe the top of the Control Center downward to hide it.

iOS uses a common set of touch-motions in its general navigation to simplify user access. For example, pinching in and out on the screen will zoom (pinch fingers inward to zoom out, pinch outward to zoom in), while double tapping will reset the zoom back to default. It helps to become adept with basic touchscreen functionality (tapping, double-taps, long-press or tap-and-hold, swipe, pinch or spread). Check out [Apple’s list of gestures](#) and helpful videos. An easy-to-understand cheat sheet for iOS can be found at [Dummies.com](#), the folks who bring us the popular “For Dummies” series of reference books. It provides tips, tricks, and ways to get support while interpreting the most common icons, navigation, and screen operations.



Use strong passwords. Increase the effectiveness of a password by adding numbers, symbols, and mixed-case letters. Avoid easy-to-guess information or personal information (like birth dates or the word “password”), and update them every six months.

Use tracking and control apps if iOS doesn’t offer enough protection. Consider [OurPact](#), [Norton Family Premier](#), [FamilyTime](#), and others. Some apps even contain regularly updated algorithms to alert parents of signs of depression, online predators, bullying, sexting, school safety threats, pornography, and harmful online content. Internet browsers (like Google Chrome and Mozilla Firefox) also offer their own filtering systems; research free browser filters with [this reference from Common Sense Media](#).

Observe the teen, and trust your instincts. It’s easy to get caught up in the accusations and generalizations made about teen media and device usage, but no one really knows a kid better than his/her parent. The level of digital privacy appropriate for a teen depends on his/her personality, behavior, emotional development, well-being, social activity, and their ever-changing desire for freedom. A teen who behaves in a socially balanced way, maintains an honest relationship with her family, and primarily uses tech as a tool may require less monitoring on his/her device than one who is naturally shy and tends to socially isolate. Similarly, a parent may need to limit the digital privacy of a child who struggles with authority figures, while another parent may allow a 13-year-old to take a smartphone with him on the bus when he travels to soccer tournaments but not to school.

Know all account names and passwords. Every teen must understand they cannot expect absolute privacy on their devices, and parents are always well within their rights to observe and monitor their children’s tech usage. Any indication that a child may hurt themselves or someone else warrants a complete review of their digital presence. Parents need complete access to the teen’s device and everything on it. Near the end of this Parent Guide, we’ll give ideas about how to partner with our kids to do this well, i.e., how to maximize the benefits and minimize the relational damage.

A Manhattan psychotherapist [shared this story](#) about kids and digital privacy:

A lot of kids who come into therapy will say their mom is always texting them and asking where they are. Interestingly, I’ll say, “How about your mom won’t hound you, or embarrass you in front of your friends, if you let her use a tracker.” They don’t skip a beat and immediately say okay, he says. Plus, he adds, if a kid is “dead against” the tracker, that could be a sign that something’s wrong.

Is it possible to completely protect a teen from risk or to prevent access to undesirable content via their iOS device?

Unfortunately, no. What's possible and much more effective, though, is to teach teens respect for the technology, to disciple them into a healthy habits, and to take an active, teachable, listening attitude toward what's important to them. After all, it may seem a teen cares more about the device than anything else, but remember the real value is in the connection facilitated by the device to their identity, their friends, their family, and their future—the stuff everyone *really* cares about.

As imperative as it is to keep our teens safe and healthy, we will needlessly damage our relationship with our kids by constantly monitoring tech use simply out of curiosity or asymptomatic worry (or control), especially when we use controls without the teen's knowledge or buy-in. Ultimately, this practice will encourage more sneaking around and undermine the development of important character traits like responsibility, trust, self-discipline, and honesty. Deceitful parenting places a child in severe physical and emotional jeopardy like nothing else, and as we said, we just can't depend on tech alone to keep our kids safe.

The best results come from managing a device's operating system in combination with vigilant observation and proven relational techniques. These include open discussion, complete disclosure, appreciation of all points-of-view, acknowledgment of good behavior, reasonable expectations, and regular check-ins as agreed. As you implement boundaries, ask God to give you discernment of what boundaries work best for each child, when to trust a child vs. when they're not being honest, and when to add or revoke more privileges. And yes, it's ok to pray that your child will get caught in their sin!

In this way, we change what seems like an overwhelming parental responsibility into an opportunity. We get the chance to “train up a child in the way they should go” ([Prov 22:6](#)), and our kids get the chance to “set an example in speech, in conduct, in love, in faith and in purity” ([1 Tim 4:12](#)). It's definitely a win-win.

The bottom line

No parental control algorithms, settings, or apps are a good substitute for you, the parent. You know your kid best and therefore can make the best decisions for them as to when to get a smartphone, how to implement controls and monitors, how to create an atmosphere of accountability, and how they can earn more freedom and responsibility (yes, despite what they think, you do know better than they do).

We've all heard the old adage, “Do as I say, not as I do,” but research shows that our children are formed far more by what we actually do than what we say. Also, the effects of our teaching diminish when we ourselves don't practice what we preach. Your teens will be much more likely to understand and submit to boundaries and accountability if they first see you submitting to them as well; that's why modeling appropriate behavior with our smartphones is so critical. None of us is immune to temptation. We all need accountability and, at times, help resisting temptation, especially when it comes to devices like smartphones that are [designed to be addictive](#). We have a unique opportunity to set a precedent for our teens by being vulnerable, having regular accountability checks, and submitting ourselves to the same (or similar)

boundaries to which we submit them.

Pair this with having tough-but-powerful conversations about why you make the decisions you make and how they feel about those decisions. ***Inviting open, honest dialogue is the absolute best thing you can do for your kids.*** The more they feel heard and understood, and the more you can help them see the heart behind your decisions, the more likely they are to (eventually) see the wisdom and submit to your authority.

But the opposite is also true: The more we simply enforce rules with no explanations, the more we restrict, the more we focus on good behavior rather than their hearts, the more likely our kids are to disobey, rebel, and do what they think is best—to their own harm and heartache, of course.

The best gift we can offer our kids is an open, honest relationship, one that's built on trust, responsibility, love, and the Gospel. Smartphones are simply part of that relationship—not the enemy—and we have an opportunity to disciple our kids into a biblical perspective of their phones and how they should fit into their lives.

Note: We highly recommend also reading our “Parent’s Guide to Smartphones” for tips on how to view smartphones, how to prepare a child for getting his/her first smartphone, and more.

Additional resources

[Everything You Need to Know about Parental Controls](#), from Common Sense Media

[How to Set Up Parental Controls](#), Apple.com

[Parental Controls: The Ultimate Guide](#), iMore.com

[A Parent’s Guide to Smartphones](#), Axis.org

[A Parent’s Guide to Sexting](#), Axis.org

[A Parent’s Guide to Instagram](#), Axis.org

[A Parent’s Guide to Snapchat](#), Axis.org

[A Parent’s Guide to Internet Filtering](#), Axis.org (coming soon!)

We’re creating more content every day! If you found this guide helpful and valuable, check out axis.org/guides each month for new Guides covering all-new topics and for other resources.