

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

Android

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

Android: Phone or Sentient Robot?

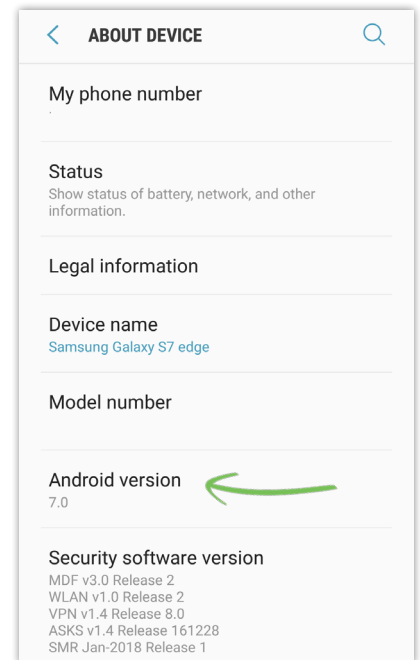
21st-century parents have to figure out all kinds of digital technology, even if we're not particularly "techie" by nature. It's similar to when we worry about helping a high-schooler with algebra when we ourselves are lousy at math. We can send them to tutors when they grow beyond our experience in 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 > About Device (see photo).



What should I know about Android OS?

Android OS, by far the most-used mobile operating system on earth, controls [more than 80% of the mobile OS market](#). The Apple OS (known as iOS) makes up the rest. As we mentioned, there are others, but no other system even comes close to the Android in terms of popular usage. More than a billion smartphones containing the Android system [shipped in 2016 alone](#), and while the iOS works on about 60 devices, more than [18,000 different Android-compatible devices](#) exist.

Android's widespread usage results from its "open-source" format, which makes it compatible with an enormous variety of features and apps. Any hardware manufacturer can build a device to run the Android OS, unlike iOS, which strictly limits compatibility to their own products.

With respect to parenting, the online buyer's guide [Laptop Mag](#) insists [Android offers superior parental controls](#) to those offered by Apple's iOS. Their reasoning: iOS provides some basic tools

limited to Web-content blocking, but Android's open-source OS allows developers of protection options more creativity and deeper access. Parents can manage the entire device's operation, instead of just individual functions, apps, or browsers. Many Android devices come standard with 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.

— How do I set up parental controls on an Android device?

In an ideal situation, parents set themselves up as the primary user on an Android device, then add the teen as a secondary user (though some Android manufacturers have disabled this feature, so check online to see if your specific device offers this). This allows the teen to customize it, including the installation of wallpapers or apps, without changing the device's primary functionality or limits. On Android OS, the second user will need a Google account, which can be created while setting up the secondary user profile.

Parents can also implement controls on individual Android services—pre-installed on all Android devices—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.

Android also offers a photo sync function that backs up photos to Google automatically; some parents find this a convenience, but it can make the photos vulnerable to information-thieves and predators. (A teen's photo collection provides personal information about his/her habits, friends, hobbies, schedule, hangouts, and other details helpful to predators in striking up a conversation, showing interest, aligning themselves with a child's favorite things, and eventually gaining trust.) Parents can decide whether to use the sync function to review the photos taken on the device, or if they'd prefer to turn the function off to restrict access.

As mentioned, Android's "open-source" system can host a huge variety of downloads from sources other than the Play Store. The following instructions show how to regulate these third-party downloads.

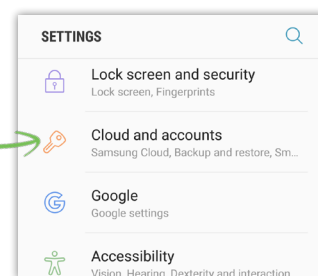
Note: Because not all Android devices are set up in the same way, your device may differ from these instructions. If so, simply search online for your device's name, the operating system, and the function you're trying to complete.



(or similar) = Settings app

Add a [secondary user](#):

1. Tap the **Settings** icon to open the menu.
2. Tap **Users & Accounts** (or **Cloud & Accounts**, depending on the device). The accounts already added to the device should now be visible.
3. Tap **Add User**. The system will provide instructions on how different user accounts work. Tap OK after reading them, then tap **Set Up Now**.
4. Unlock the phone, if necessary. The system will then provide more




important information to know about setting up secondary users; tap **Continue** after reading these.

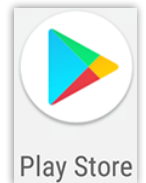
5. Enter the email and Google password for the second user. (If the user does not have a Google account, tap **More Options** to create it for them.)
6. Read the information given and tap **I Agree**.
7. A list of Google services will appear. Tap applicable **checkboxes** to add or remove options, then press **Agree**.

Switch between users:


1. **Swipe down** from the top of the device's home screen.
2. Locate and tap the appropriate icon (it's a white silhouette of a person on a colored circle).

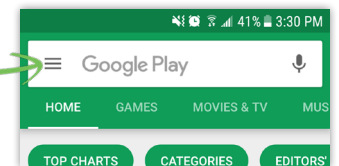
Regulate use of the App Store:

3. Access the appropriate user account (see above).
4. Open the **Play Store** (it's a multicolored triangle icon, right). 
5. Tap **Menu**, then **Settings**.
6. Tap **Parental Controls**, then tap the switch to activate them.
7. Choose a PIN, tap OK, type it again, then tap **Continue**. This prevents alteration of the controls by anyone but the primary user.
8. Age-ranges may now be set for each content type, or content may be restricted altogether, as you choose.



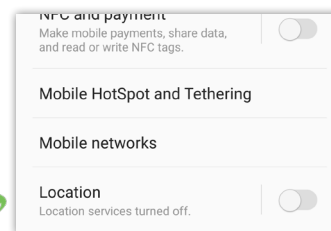
Require a PIN for purchases:

1. Open the **Play Store** and tap the **Menu**  icon.
2. Tap **Require Authentication for Purchases**. Choose how often authentication will be necessary to buy anything on the device.





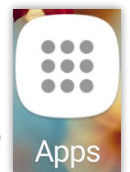
Turn location services on or off:

1. Tap **Settings**, then tap **Security & Location**.
2. Turn **Location** on or off, as desired.




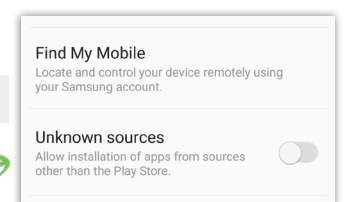
Turn photo sync on and off:

1. Open the **app drawer** on the device (see photo). 
2. Swipe through the app collection to find **Photos** or **Google Photos**. Tap to open the app.
3. Tap the **Menu** icon  (typically three horizontal lines in the top-left corner of the screen, often referred to as the "hamburger") to open the left sidebar.
4. Tap **Backup & Sync** to turn the function off and on (it will turn blue when it's on).



Regulate downloadable apps from other sources:

1. Tap **Apps**, then **Settings**, then **Security** (or **Settings** then **Lock Screen & Security** on Samsung devices).
2. Tap the **Unknown Sources** switch to turn it off (left, no color) and on (right, color). 



— 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 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.

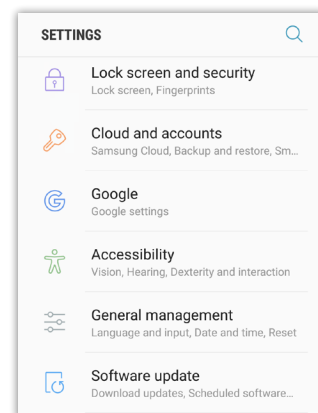
Finally, we must remind our teens that while we parents are paying for the phones and they're living under our roofs, *they* don't own the devices; we do. So if they continue to abuse their phone privileges, then we will continue to revoke those privileges until they can regain trust and prove that they're 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 out of Android OS?

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.

Android OS offers regular, automatic updates. When notices of these appear on the device, simply agree to install them as instructed in the notification. Users can also check for updates manually under **Settings** by choosing **System Updates**, then **Check For New System Update** (see photo; again, this varies by device).

Learn the navigation system. The Android OS uses a common set of cross-functional icons to simplify user access. For example, a vertical



set of three dots indicates a list of actions (like a menu), a star-shape indicates a “favorite,” and the “hamburger” icon opens the navigation tools on most Android apps. It also helps to become adept with the Android touchscreen functionality (tapping, double-taps, long-press or tap-and-hold, swipe, pinch or spread). Here’s an [easy-to-understand cheat sheet](#) for Android OS written by the people 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 Android OS doesn’t offer enough protection. Android’s open-source format makes hundreds of parental control apps available for download, many more than any other operating system. Consider Google’s [FamilyLink](#), [Bark](#), [TeenSafe](#), 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 your 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. As mentioned, a parent can best monitor and manage the use of a smartphone or other mobile device when he/she is designated as the device’s primary user. The parent can then create a secondary user profile for the teen while managing overall access to content, downloads, apps, purchases, callers, texts, and pretty much anything else via the device.

If this designation isn’t possible or optimal, however, parents need complete and regularly updated 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 Android 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 Android Parental Controls](#), TeamKnowHow.com

[Here’s How Google’s Parental Controls for Android Work](#), Fortune.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.