Safeguarding Our Children:

Key Strategies for Navigating Technology with Your Teens

GREEN ZONE: Here are the few apps considered to be safe for Teens and Tweens: The internet can be a dangerous place for teens. However, these apps are the "lesser of three evils" as they can be used to help a student (14+ years of age) shine online to impress colleges and future employers. It's not to say that situations cannot arise from children using these. When used wisely, these apps will help your students adjust their Google results to create a portfolio of positive online accomplishments. If your students want to have a profile on these networks/apps, please consider having a dialog with them and knowing that these networks are the place to start on social media. On following pages there is a list of bad apps (red zone) that you might not allow your kids to access/have/use.

Facebook

Age: 13+
Facebook aims to give people the power to share and make the world more open and connected. Kids tend to share personal information on their Facebook profile.This information is often visible for college admissions officers, and future employers when they search for them. Watch our video.

Facebook Messenger

Age: 13+
Facebook messenger (owned by Facebook) allows you to chat with anyone on Facebook. To initiate a conversation with users you need to add them to your Facebook friend list. We suggest parents to add their students on Facebook and monitor who they are adding as friends. Watch our video.

Instagram

Age: 13+
Instagram is a free photo sharing application that allows users to take photos, apply a filter, and share it on the service or other social networking services. This app is great for showcasing one's accomplishments and adventures. However, kids need to be careful with what pictures they do post. Watch our video.

LinkedIn

Age: 14+
LinkedIn is the world's largest professional network. It is an important tool for teens that want to improve their Google results when applying to college. It is the best place to start an online image to impress colleges and future employers. Watch our video.

Pinterest

Age: 13+
Pinterest is a visual discovery tool that helps users find and save ideas. It's a great source of inspiration for students. They can use Pinterest to find studying tips, DIY's and more. Kids can have fun on Pinterest, as long as they pin pictures that are Light, Bright and Polite. Watch our video.

Twitter

Age: 13+
Twitter is an online social network, which allows you to send messages up to 140 characters in length. This is a great app for students to share their thoughts and feelings. However, kids must also be aware that anyone can view what is posted if their account is public. Watch our video.

YouTube

Age: 13+
YouTube is a free platform for watching and uploading videos, and is owned by Google. Positive videos can turn a student's Google results into a three dimensional version of their college resume. YouTube also has a multitude of educational videos you can learn from. Watch our video.

GRAY ZONE: These apps can be good (and bad) for your Teens and Tweens. Its recommended you have a dialog with your kids about Sexting and inappropriate content if your kids have these apps. Although some people are very scared of Snapchat and Vine, there are way worse apps that your kids could be using. It's suggested every parent put in the time each month to have a dialog with their kids about the apps they are using. This is the best way to keep your kids safe (not by restricting the kids, but by talking with them).

Musical.ly App

Age: 13+
Musical.ly is a popular app that let's users create lip-syncing videos to their favorite songs. While this app may be fun for teens it may be scary for tweens due to the adult content that can be found on this app. Watch our video.

Periscope App

Age: 13+
Periscope is a location based app. It allows users to watch and broadcast real time videos. It's easy to find your kids on Periscope if you know their Twitter usernames. Some teens get in trouble using the Periscope app. Watch our video.

Pokémon Go

Age: 9+
Pokémon Go is an augmented-reality mobile game for iOS and Android devices. While quickly becoming one of the most popular apps of all time, it has raised some safety concerns. Learn how your kids can have fun and still stay safe if they play Pokémon Go. Watch our video.

SMS Text Messaging

Age: No age limits
SMS text messaging is one of the primary apps that each phone has. All accounts are connected to phone numbers. SMS messenger is relatively safe for students – trackable and least difficult for parents to monitor. Watch our video.

Snapchat App

Age: 13+
Snapchat is a messaging service that allows people to send photos and short videos to each other that disappear seconds after opening them. A major concern with Snapchat is how teen Snapchat users use the app, since parents are not on it and content disappears. Watch our video.

Vine App

Age: 17+
Vine is owned by Twitter and is a video sharing app. Kids often post videos of their everyday life and blunders. Kids want popularity, so they try to collect more views and revines from friends and strangers. Watch our video.

WhatsApp Messenger

Age: 16+
WhatsApp is a mobile messenger that is similar to short message services. Users can share location and contacts with other users. WhatsApp helps kids bypass text messaging and communicate with their friends using the app. Watch the video.

RED ZONE: ANONYMOUS APPS – Here are the apps we consider to **NOT** be safe for Teens and Tweens.
These are the apps not recommended for Teens or Tweens. These apps usually have inappropriate and unmoderated content. Also, they lend themselves to cyberbullying. Often, these apps are anonymous and will encourage students to behave in a way we have never seen before. When students use an app in anonymous mode (without it being tied to their real identity) they tend to behave badly. They are also more prone to bullying and predators in this zone.

AfterSchool App

Age: 17+
AfterSchool App is an anonymous app that creates a separate chat group for every school. It has been removed twice from the AppStore because of threats and arrests. Messages often include bullying, pornography, and alcohol or drug references. Watch our video.

Ask.fm

Age: 13+
Ask.fm is a social networking website where people can ask questions, with the option of anonymity. Kids often reveal too much personal information on this site, and cyberbullying is very prevalent. Watch our video.

BurnBook App

Age: 18+
BurnBook is an anonymous app for posting text, photos and audio rumor messages about others. The app compiles messages by school, so the app requires access to your location. It encourages students to screenshot the rumors and save them to their phone, which causes bullying issues. Watch our video.

Calculator% Private Photo App

Age: 4+
The “Private Photo (Calculator%)” app is designed to help students hide photos and videos behind an innocent looking calculator app. This application looks like a calculator but entering a passcode opens a private area. Watch our video.

Finstagram App

Age: 13+
Finstagram (Finsta) is a fake (or second) Instagram account. Students get a second Instagram account along with their real Instagrams (Rinstagrams), to post silly pictures or videos. Watch the video.

Kik Messenger App

Age: 17+
Kik allows anyone on the app to contact your child and directly message them. It has been known to allow adults to communicate with preteens, and is very difficult to discern who is a predator and who is real. Some adults have been known to use this app to pretend like they are tweens and teens. Kik allows students to bypass text messaging features of their phone. Users can connect with anyone on the network and aren’t limited to their phone’s contact list. Watch the video.

Ogle App

Age: 17+
Ogle is an anonymous app that automatically searches your location for nearby schools when downloaded. View and interact with school feeds, engage on any campuses content, and share or ask anything anonymously. Since there is little formal registration, bullies and predators can easily masquerade as students and friends. Watch the video.

ooVoo App

Age: 13+
ooVoo is one the world’s largest video and messaging apps. Parents should be aware that ooVoo is used by predators to contact underage kids. The app can allow users to video chat with up to twelve people at one time. Watch our video.

Secret App

Age: 17+
Secret is an app that allows people to share messages anonymously within their circle of friends, friends of friends, and publicly. Students often hide behind the anonymity when posting, and forget that anonymous does not mean untraceable. Watch our video.

Slingshot App

Age: 13+
Slingshot is a comparison app, marketed to boys, that allows users to vote or create polls. Slingshot users can create any type of poll, including polls that are not appropriate for teens. This app is popular with students, and the comment section is used to bully other students.Watch our video.

StreetChat App

Age: 14+
StreetChat is a live photo-sharing board designed for middle school, high school and college students. Kids feel more freedom to send mean posts because they do not have to confirm their identity within the app. This leads to students often posting about real people. Watch our video.

Tumblr

Age: 13+
Tumblr is one of the world's most popular blogging platforms. Users tend not to use their real names, so it can be hard to find blogs without knowing a specific username. All accounts are public and content goes unmonitored. Watch our video.

WhatsGoodly App

Age: 17+
WhatsGoodly is an anonymous, location-based, social polling application designed for college students. It has a 17+ age restriction, but younger students can still see polls and vote. There are a lot of questions about dating, relationships, alcohol, and smoking on the app. Watch our video.

Whisper App

Age: 17+
Whisper is an anonymous social network that allows people to express themselves. Whisper reveals a user's location, which makes it easy for people to arrange to meet up. This also makes it easier for predators to locate and connect with users. Watch our video.

Poof App

Age: 17+
text messages that automatically POOF (disappear) after they've been read!
When you send a POOF text message, it's automatically deleted off your phone. When you read a POOF text, it too is instantly deleted off your phone. POOF text messages are never stored on servers, and leave no text messaging footprint behind!

Yik Yak App

Age: 18+
Yik Yak acts like a local bulletin board for your area by showing the most recent posts from other users around you. The app is popular with high school students, and it is often used to harm the self esteem of fellow students. Watch our video.

YouNow App

Age: 13+
YouNow is a popular broadcasting platform where kids watch and stream real-time videos. Users decide whether broadcasters should continue their live videos with thumbs up and thumbs down voting. Anyone can record the videos posted, take screenshots and bully others with the recordings.
Watch our video.

IT'S IMPORTANT TO LOOK AT YOUR CHILD'S DEVICE.

Wishbone App

Age: 13+
Wishbone is a comparison app, marketed to girls, that allows users to vote or create polls. Wishbone users can create any type of poll, including polls that are not appropriate for teens. This app is popular with students, and the comment section is used to bully other students.Watch our video.

What Should You Do As a Parent

Monitor your child's technology use

Regardless of how much your child resents it, you can only protect him or her by monitoring what they do online.

1. Keep the computer in a busy area of your house so you can easily monitor its use, rather than allowing your child use a laptop or tablet in his or her bedroom, for example.

2. Limit data access to your child's smartphone if he or she uses it to surf the web. Some wireless providers allow you to turn off text messaging services during certain hours.

3. Set up filters on your child's computer or device. Tracking software can block inappropriate web content and help you check up on your child's online activities.

4. Insist on knowing your child's passwords and learn the common acronyms kids use online and in text messages.

5. Talk to your child about the people they communicate with online. Go over your child's address book and instant messenger "buddy list" with them. Ask who each person is and how your child knows them.

6. Encourage your child to tell you or another trusted adult if they receive threatening messages or are otherwise targeted by cyberbullies, while reassuring them that doing so will not result in their loss of computer or cell phone privileges.

7. **Know the apps that are on your child’s device.**

New apps come out everyday, So be smart, be informed, and pay attention.

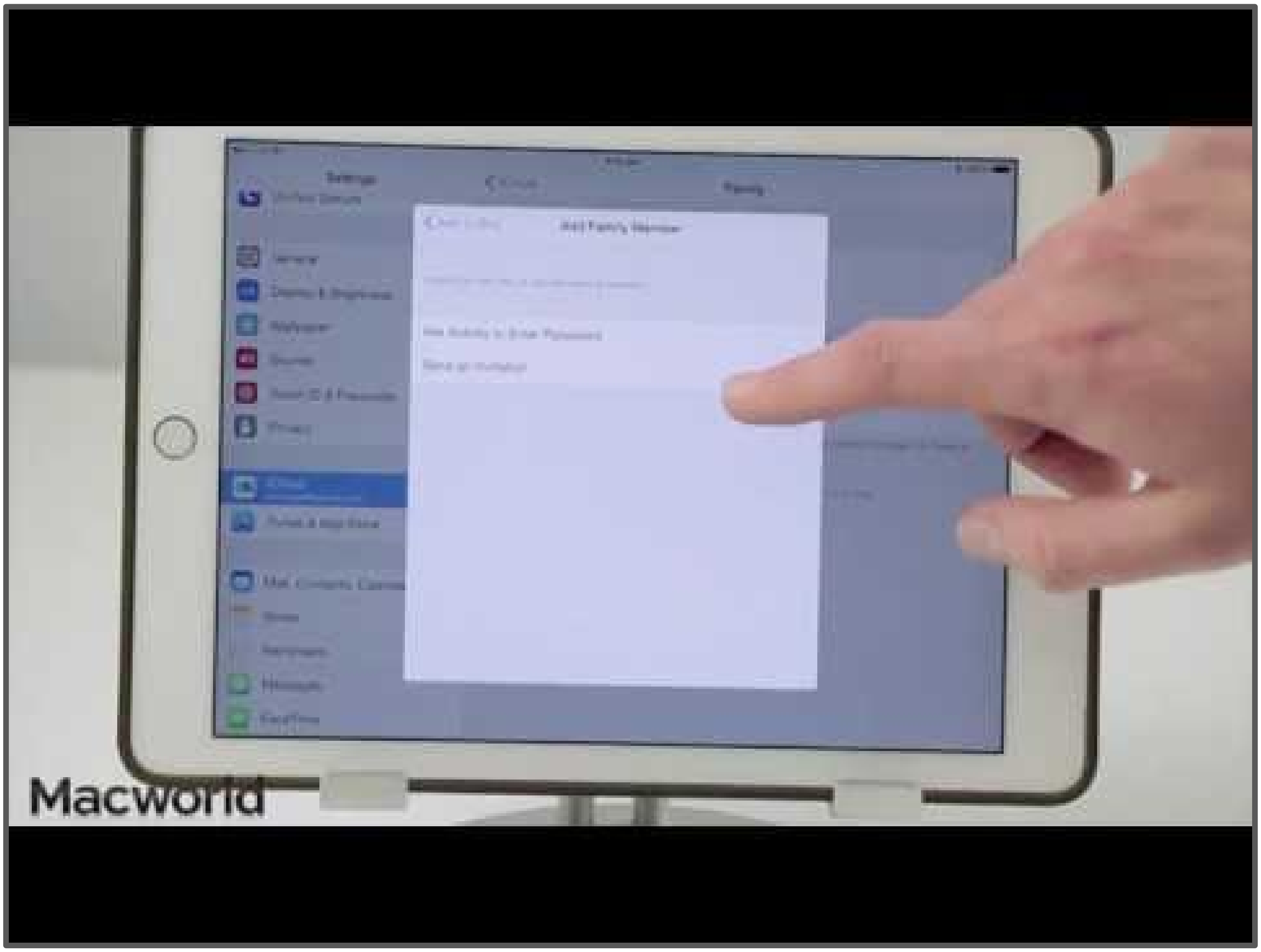
Managing your Apple Devices with **Family Sharing**

Family Sharing. Bring harmony to your family's digital life.

Family Sharing makes it easy for up to six people in your family to share each other's iTunes, iBooks, and App Store purchases without sharing accounts. Pay for family purchases with the same credit card and approve kids' spending right from a parent's device. Share photos, a family calendar, and more to help keep everyone connected. And with an Apple Music family membership, up to six people can get full access to Apple Music, too.

Learn more at:
http://www.apple.com/icloud/family-sharing/

How to Setup Family Sharing on iPad and iPhone

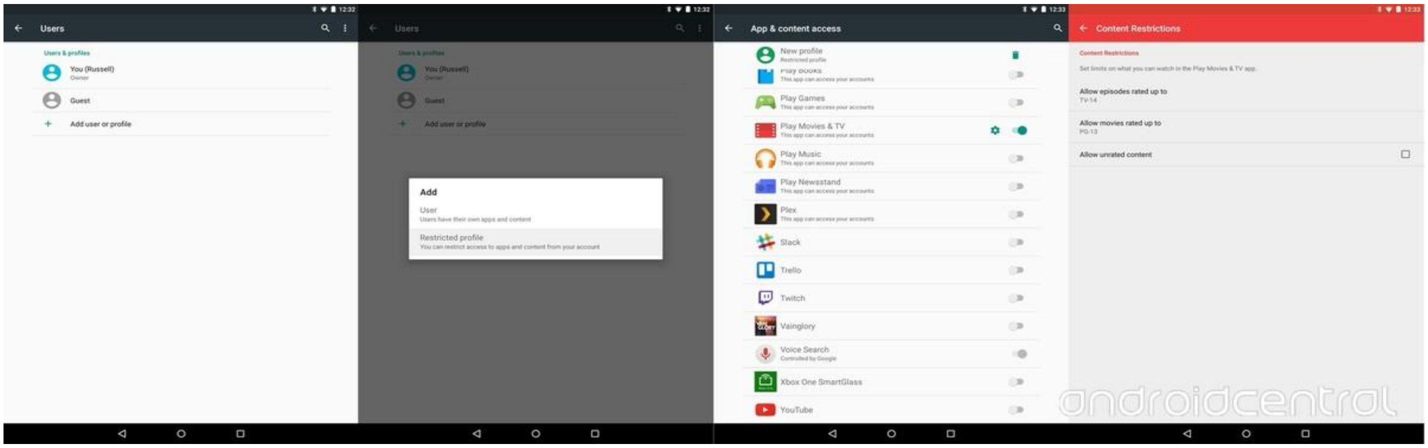


https://youtu.be/TlfQeT2reJM

Setting up a kid-friendly Android device

Here's a quick tour through those steps, and some tips on keeping your child safe through Android.

Creating a new account, if you can



Users

Users & profiles

You (Russell)
Owner

Guest

Add user or profile

Add

User
Users have their own apps and content

Restricted profile
You can restrict access to apps and content from your account

App & content access

New profile
Restricted profile

Play Books
This app can access your accounts

Play Games
This app can access your accounts

Play Movies & TV
This app can access your accounts

Play Music
This app can access your accounts

Play Newsstand
This app can access your accounts

Plex
This app can access your accounts

Slack

Trello

Twitch

Vainglory

Voice Search
Controlled by Google

Xbox One SmartGlass

YouTube

Content Restrictions

Content Restrictions

Set limits on what you can watch in the Play Movies & TV app.

Allow episodes rated up to
TV-14

Allow movies rated up to
PG-13

Allow unrated content □

The easiest way to set a device up for a child is to set yourself up as the primary user and add your child as a restricted account. Primary accounts have admin controls over restricted accounts, which means you can select what apps are a part of their interface and control the kind of content some of those apps show your child. These accounts can be as open or as locked down as you choose, and you can make changes in either direction whenever you choose.

To get started, head to Settings>Users>Add user or profile. Make sure you select Restricted Profile in the options that pop up, and you'll be able to toggle on or off all of the apps you want this account to have access to. Some apps will have a gear next to the toggle, which means there are extra setup options. Google Play Movies, for example, lets you set content ratings for purchases and viewings.

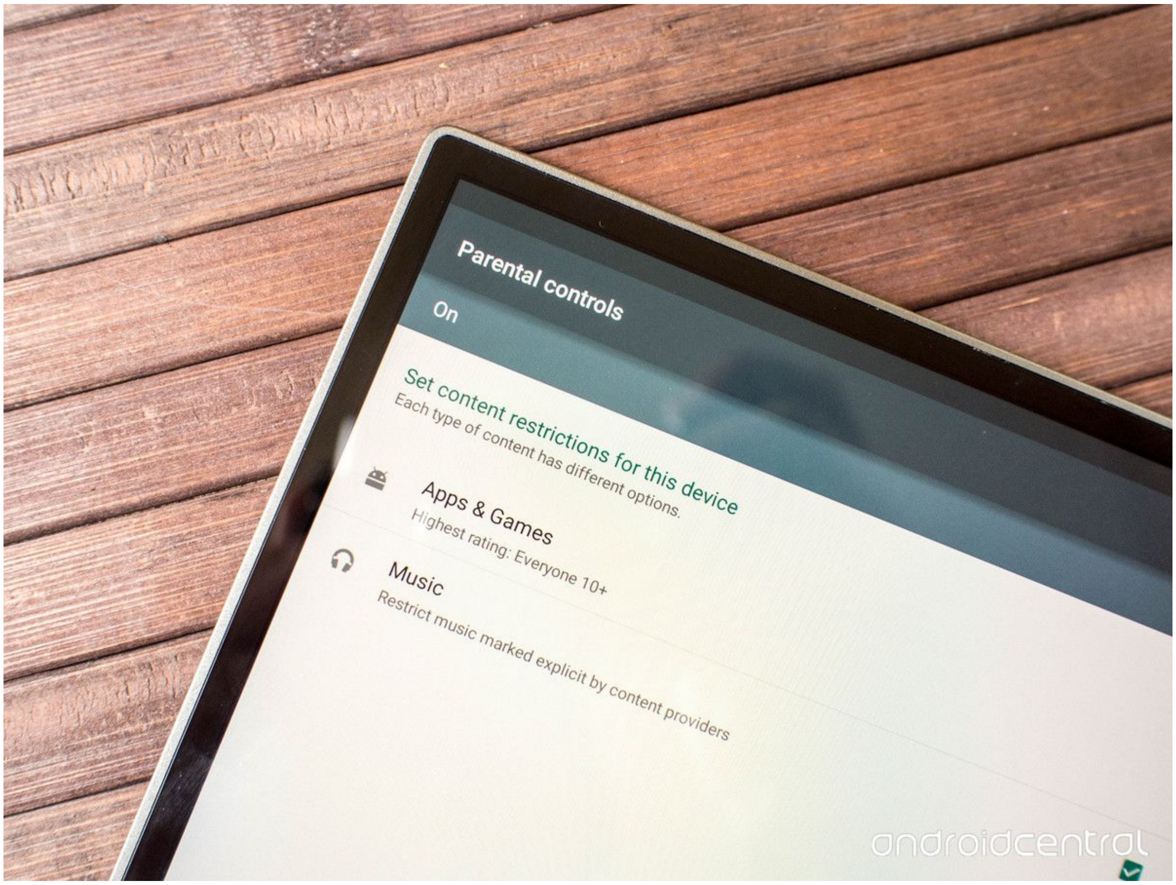
Creating a Google account and attaching your child's name to it is a personal choice.

Once these basics have been established, you can decide whether to add or create a Google account for this account. Google has a single account for everything, including apps, email, and their social network.

Creating that account and attaching your child's name to it is a personal choice, but in doing so you make it possible for your child to decide what apps they want to install and what music and movies they want to enjoy without that data spilling onto your account and altering Google's recommendations for you.

Depending on what device you use, especially if you decide to grab a Wifi-only phone instead of a tablet for your child, this particular feature may not be available. Restricted profiles were only introduced in smartphones with Android 5.0, and many manufacturers have opted out of including the feature in this generation of devices. If you've got the feature, it should absolutely be one of the first things you enable.

Kid-friendly Google Play



Parental controls

On

Set content restrictions for this device

Each type of content has different options.

Apps & Games

Highest rating: Everyone 10+

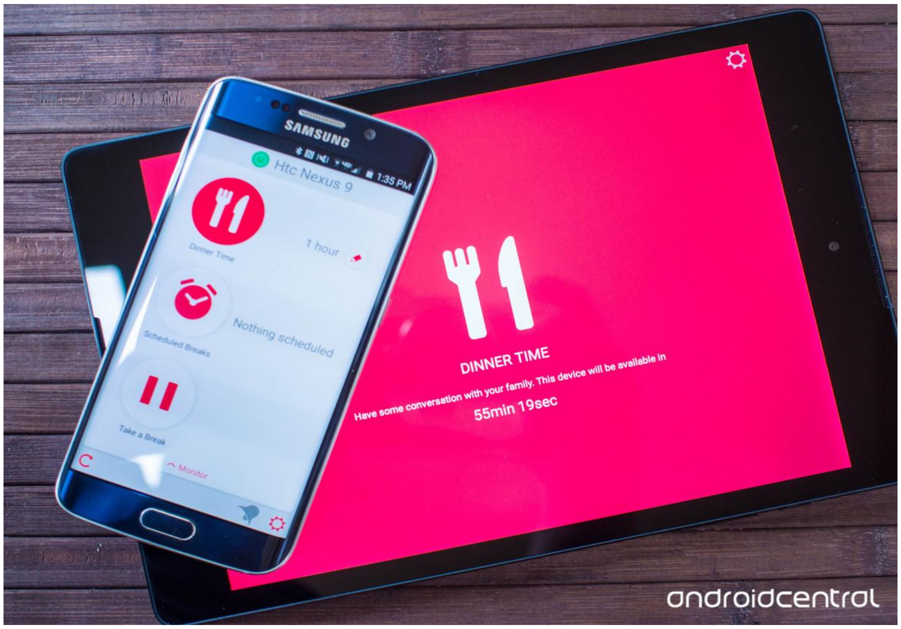
Music

Restrict music marked explicit by content providers

If you've decided to give your child access to Google Play, there are some extra buttons you can press to ensure only age-appropriate content shows up in the Play Store. Parental controls are located in the Play Store app, under Settings>Users, but you'll need to be logged in to your child's account to activate them. You'll be prompted to create a pin lock so your child can't just turn these features off, and once that is complete you'll be able to set rating limitations for Play Store apps and explicit music from the Play Music app.

Google Play Store Settings also lets you set restrictions for the ability to pay for things, assuming you aren't just limiting your child to a gift card or similarly limited payment system. Just under Parental controls in the Settings list you'll find Require authentication for purchases, which lets you choose when Google prompts you for a password. These settings can be adjusted so a password is requested every time, once every 30 minutes, or never. While this is a personal choice, setting it for every time dramatically decreases the chances for an "accidental" purchase in the Play Store.

Increased control through parent apps



Gaining additional control of your child's Android experience requires some help from third-party apps. There's no shortage of great apps to choose from when it comes to monitoring the mobile experience from another device, but the absolute best of the free solutions out there is DinnerTime Plus.

The app is designed to let the parent monitor activity from their personal device, and make changes remotely. As the name suggests, you can even hit a button that flashes a bright red screen on your child's device, letting them know it's time for Dinner and to put the gadget down.

As cute as the bright red auto-parenting tool is, the core functionality in DinnerTime Plus can be found in the reports the app generates and the control you as a parent are given over specific apps. If restricted accounts aren't an option for you, being able to block apps is the next best thing. It's also pretty useful to be able to set specific times for when the device can't be used, and have a report generated to let you know when apps are being used and for how long. It's the kind of thing Google may never make a native part of the OS, but as a parent can make a huge difference in how your child interacts with technology.

The Top Chat Acronyms Teenagers Use and Parents Should Know

1337 - Elite -or- leet -or- L337
143 - I love you
182 - I hate you
420 - Marijuana
459 - I love you
ADR - Address
AEAP - As Early As Possible
ALAP - As Late As Possible
ASL - Age/Sex/Location
CD9 - Code 9 - it means parents are around
C-P - Sleepy
F2F - Face-to-Face, a.k.a. face time
ILU - I Love You
KOTL - Kiss On The Lips
KFY -or- K4Y - Kiss For You
KPC - Keeping Parents Clueless
LMIRL - Let's Meet In Real Life
MOOS - Member Of The Opposite Sex
MOSS - Member(s) Of The Same Sex
MorF - Male or Female
MOS - Mom Over Shoulder
NALOPKT - Not A Lot Of People Know That
NMU - Not Much, You?
P911 - Parent Alert
PAL - Parents Are Listening -or- Peace And Love
PAW - Parents Are Watching
PIR - Parent In Room
POS - Parent Over Shoulder
RU/18 - Are You Over 18?
RUMORF - Are You Male OR Female?
S2R - Send To Receive
SorG - Straight or Gay
TDTM - Talk Dirty To Me
WUF - Where You From
WYCM - Will You Call Me?
WYRN - What's Your Real Name?
zerg - To gang up on someone

Visit: https://youtu.be/iBqoOf-jIKA

Resources:

Safe, Smart & Social
Teaching Students How To Shine Online

androidcentral

Tips For Dealing With Cyberbullying

DITCH THE LABEL YOUR WORLD. PREJUDICE FREE .

1. **Never respond** to anything that has been said or retaliate by doing the same thing back. Saying something nasty back or posting something humiliating in revenge may make matters worse or even get you into trouble.

2. **Screenshot** anything that you think could be cyberbullying and keep a record of it on your computer.

3. **Block and report** the offending users to the appropriate social media platform.

4. **Talk about it**. You may not feel it at the time, but you seriously are not alone. Talking to somebody about bullying not only helps you seek support but it documents evidence and will take a huge weight from your shoulders.

5. **Assess how serious** the cyberbullying is. If it is light name calling from somebody that you don't know, it may just be easier to just report and block that user.

6. **Report it**. If you are experiencing cyberbullying from somebody you go to school or college with, report it to a teacher. If somebody is threatening you, giving out your personal information or making you fear for your safety, contact the Police or an adult as soon as you can.

7. **Be private.** We recommend that you keep your social media privacy settings high and do not connect with anybody who you do not know offline. People may not always be who they say they are and you could be putting you and those that you care about the most at risk.

Tips For Dealing With Sexting

It may feel awkward, but it's important to explain to children the risks of sexting, how to stay safe and remind them that they can talk to you if something ever makes them feel scared or uncomfortable.

What is sexting?

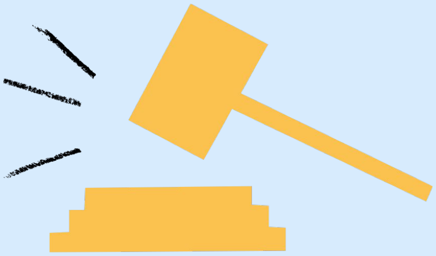
Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages.

They can be sent using mobiles, tablets, smartphones, laptops - any device that allows you to share media and messages.

Sexting may also be called:

- trading nudes
- dirties
- pic for pic.

What the law says



Sexting can be seen as harmless, but creating or sharing explicit images of a child is illegal, even if the person doing it is a child (under16). A young person is breaking the law if they:

- take an explicit photo or video of themselves or a friend
- share an explicit image or video of a child, even if it's shared between children of the same age
- possess, download or store an explicit image or video of a child (under 16), even if the child gave their permission for it to be created.

Rethink Cyber Safety Rules and the "Tech Talk" with Your Teens

staysafeonline.org

StaySafeOnline.org
Powered by National Cyber Security Alliance

stopthinkconnect.org

While NCSA believes rules still play an important role in helping young people stay safe and more secure online, we recommend revising the approach to online safety rules and taking the following into consideration:

- **Make rules that can be enforced:** It's easy to create a laundry list of rules. Making rules that are impractical to follow or enforce won't make young people safer or more secure and can create a situation where rules lose meaning and parents become disengaged. For example, as a majority of teens have online accounts that their parents aren't aware of, rules requiring advance permission before creating accounts are likely to be broken and unenforceable. Before setting a rule, think about whether it will significantly improve your children's safety and how you can keep the lines of communication on the issue open.

- **Have a core set of rules the whole family follows:** The most impactful rules are those that apply equally to everyone. So create a set of rules that everyone in the family is expected to follow. For example, limiting use of devices during meal times or other times spent together as a family, practicing discretion when sharing personally identifiable information about family members, and seeking permission from one another before sharing information, such as posting photos on social networks.

- **Make rules together and change them over time:** Young people may surprise you with how much they already know about being safer and more secure online. Ask them about the rules they have made for themselves and the practices they currently follow. Then have them establish rules they can commit to following. Make sure that the rules evolve as your children grow. What is an appropriate rule for a 10-year-old may not be appropriate for a teen, so periodically revisit your expectations.

It's not about the technology - it's about how it is used.