

---

DIGITALLY UNDRESSED  
FREE TOOLKIT

# The Parent's Digital Safety Playbook

Platform-specific controls by age group with conversation scripts

Your kids are not using the internet the way you did. They live inside it. This guide gives you concrete, platform-specific settings organized by your child's age - plus scripts for having the conversations that actually work. No shaming. No spying. Just informed protection.

Estimated time: 20-30 minutes

From the book *Why Am I the Only One Naked?*

[thedreamerai.com/digitally-undressed](http://thedreamerai.com/digitally-undressed)

Share this guide freely. Privacy is not a privilege.

---

## The Reality Check

---

The average child receives their first smartphone at age 10. By age 13, most have accounts on platforms designed to maximize engagement from adults with disposable income - not protect developing brains.

Privacy settings that exist are buried, changed frequently, and designed to be confusing. In 2024, a bipartisan Senate hearing confirmed what parents already suspected: these companies know their platforms harm children and have actively chosen not to fix it.

This is not your fault. These platforms employ thousands of engineers to make opting out hard. But your child cannot wait for regulation. This guide gives you the controls right now.

---

### Ages 5-9: The Foundation

No social accounts. Device controls, content filters, and building digital awareness early.

At this age, children should not have their own accounts on any social platform. But they are already using devices - tablets for school, your phone for YouTube, shared computers. The risks are data collection and accidental exposure, not social pressure.

#### [Step 1] Set Up a Child Account - Not Your Account

- ▶ **iPad/iPhone:** Settings > Family > Add Member > Create Child Account. This enables Screen Time controls, purchase restrictions, and content filters automatically.
- ▶ **Android tablet:** Settings > Google > Parental Controls > Create supervised account through Google Family Link. Lets you approve app installs and set daily time limits.
- ▶ **Why this matters:** When kids use your account, they inherit your permissions, your search history gets mixed with theirs, and ad algorithms start targeting a profile that is half-adult, half-child. This creates bizarre and sometimes harmful content recommendations.

#### [Step 2] Lock Down YouTube

- ▶ **Install YouTube Kids** (not regular YouTube). Set the content level to "Younger" (4-7) or "Older" (8-12). Turn OFF autoplay. Turn OFF search for children under 7.
- ▶ **If using regular YouTube:** Settings > General > Restricted Mode > ON. Imperfect - blocks a lot but not everything. YouTube Kids is safer for this age.
- ▶ **What YouTube collects:** Watch history, search queries, session duration, what they skip, what makes them click. All of this builds a behavioral profile - even for young children.

#### CRITICAL

YouTube autoplay is engineered to keep viewers watching. Research has documented children going from educational content to disturbing content in as few as 3-4 autoplay hops. Turn it off.

#### CONVERSATION SCRIPT - AGES 5-9

*"Some apps try to learn everything about you so they can show you things they want you to click on. It is like if someone followed you around the store writing down every toy you looked at. We are going to set some rules so the apps cannot do that as much. You did not do anything wrong - the apps are just nosy."*

## Ages 10-13: The Critical Window

First phone. Social pressure. Your role shifts from gatekeeper to informed guide.

This is where everything changes. COPPA requires parental consent for accounts under 13, but enforcement is nearly nonexistent - most kids enter a fake birthday. The platforms know. They do not care. Your job is to set the guardrails before the pressure hits.

### [Step 3] Instagram Settings

- ▶ **Private account:** Settings > Privacy > Private Account > ON. Non-negotiable at this age.
- ▶ **Restrict DMs:** Settings > Privacy > Messages > "Only people you follow." Blocks unsolicited contact from strangers.
- ▶ **Disable activity status:** Settings > Privacy > Activity Status > OFF. No one needs to know when your child is online.
- ▶ **Turn off Suggested Users:** Settings > Privacy > "Show Account Suggestions" > OFF. Prevents strangers from being recommended your child's profile.
- ▶ **Supervision tools:** Instagram now offers parental supervision through the Family Center. Link your account to theirs for visibility into time spent and settings.

#### IMPORTANT

Instagram's algorithm treats a 13-year-old's engagement identically to an adult's. It does not moderate content intensity by age within the main platform. Teen accounts have some restrictions by default now, but verify every setting manually.

### [Step 4] TikTok Settings

- ▶ **Restricted Mode:** Settings > Content Preferences > Restricted Mode > ON. Set a passcode they do not know.
- ▶ **Private account:** Settings > Privacy > Private Account > ON.
- ▶ **Disable DMs:** Settings > Privacy > Direct Messages > "No One" (under 16) or "Friends Only."
- ▶ **Screen Time:** Settings > Screen Time > Daily Screen Time Limit. Set limit and passcode.
- ▶ **Family Pairing:** Link your TikTok account to theirs for remote control over settings - even when you are not holding their phone.

#### PRO TIP

TikTok's "For You" algorithm learns preferences within minutes. Even with settings locked down, the content feed adapts aggressively to whatever gets engagement. Talk to your child about what they are seeing, not just how long they are watching.

### [Step 5] Snapchat Settings

- ▶ **Ghost Mode:** Snap Map > Settings (gear icon) > Ghost Mode > ON. Hides your child's real-time GPS location. Non-negotiable.
- ▶ **Contact settings:** Settings > Privacy Controls > Contact Me > "Friends Only."
- ▶ **View My Story:** Settings > Privacy Controls > View My Story > "Friends Only."
- ▶ **Quick Add:** Settings > Privacy Controls > "Show Me in Quick Add" > OFF. Prevents strangers from discovering the account.
- ▶ **Family Center:** Snapchat now offers a Family Center for parental oversight. Pair your account to see who they communicate with (not message content).

#### CRITICAL

Snap Map shows your child's exact, real-time GPS location to everyone on their friends list by default. Ghost Mode is the single most important setting on Snapchat. Verify it is on today.

CONVERSATION SCRIPT - AGES 10-13

*"I am not trying to spy on you or take your phone away. But these apps are designed by huge companies whose entire business model is keeping you scrolling as long as possible and learning everything about you while you do. The settings we are changing together make it harder for strangers to find you and harder for the apps to build a profile on you. You would not hand your diary to a stranger. Your phone has more in it than any diary ever did."*

## Ages 14-17: Informed Autonomy

Education over surveillance. Shared decision-making. Building habits they carry into adulthood.

Surveillance-based parenting backfires at this age. Teens with overly monitored devices find workarounds, use friends' devices, or create secret accounts. The effective strategy is education and shared decision-making - give them the information, let them choose, verify settings together.

### [Step 6] The Quarterly Settings Audit (Do It Together)

- ▶ **Every platform - check privacy settings together quarterly.** Not as punishment. As maintenance. Like changing smoke detector batteries.
- ▶ **App permissions:** Go through their phone's permission list (camera, microphone, location, contacts) and discuss which apps genuinely need each one.
- ▶ **Connected Apps:** In Google, Apple, Instagram, and Snapchat settings, review which third-party apps have been granted access. Revoke anything unrecognized.
- ▶ **Tagged photos:** Show them how to review what others have posted that includes them. Their digital footprint is partly controlled by their friends.

#### PRO TIP

Frame this as "digital hygiene" - like brushing teeth, not a police search. The goal is a habit they carry into adulthood, not a fight they resent.

### [Step 7] Digital Footprint Awareness

- ▶ **Google yourselves together.** Search their full name in quotes. Check Google Images. Show them what a college admissions officer or employer would find.
- ▶ **Check data broker sites:** Search their name on Spokeo, BeenVerified, and WhitePages. If results appear, submit opt-out requests together. This teaches them the system is real and actionable.
- ▶ **Explain permanence:** Screenshots are forever. Deleted posts are cached. The internet does not forget - it just moves the memory somewhere less obvious. In 2025, multiple college admissions offices confirmed they review applicants' social media as standard practice.

#### CONVERSATION SCRIPT - AGES 14-17

*"I trust you more than I trust the companies that made these apps. I am not checking up on you - I am showing you what these platforms do behind the settings you can see. You are smart enough to decide how much of yourself you want to share. I just want to make sure the decision is actually yours, and not something a company made for you by burying the off-switch."*

## Universal Rules - Every Age

---

### 1. No devices in bedrooms at night

Charging station in the kitchen or living room. This is not about trust - it is about sleep, mental health, and removing the pressure to be "always available." Research consistently links bedroom device access with sleep disruption, anxiety, and reduced academic performance in children of all ages.

### 2. No accounts before the platform's minimum age

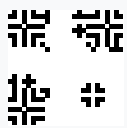
If TikTok says 13, honor it. The age gate exists because the algorithm behind it was not designed for younger brains. Lying about your child's age also means they miss whatever (limited) protections the platform does offer minors.

### 3. Settings checks are routine, not reactive

Do not wait for an incident. Quarterly privacy audits - phone in hand, side by side, no judgment. Platforms change their settings interfaces regularly. What you configured six months ago may have been reset or relocated.

### 4. Model the behavior

If you want your child to take privacy seriously, they need to see you taking it seriously. Do the Ten-Minute Privacy Cleanse on your own phone first. Let them watch. Answer their questions. Show them you believe this matters enough to do it yourself.



#### Want the complete platform-by-platform breakdown?

*Why Am I the Only One Naked?* covers 50 platforms with privacy grades, business model explanations, and step-by-step fixes for each one.

Free with Kindle Unlimited.

Scan the [QR code](https://www.amazon.com/dp/B0DQJPPKGM) or visit [amazon.com/dp/B0DQJPPKGM](https://www.amazon.com/dp/B0DQJPPKGM)