Keeping Children and Youth Safe Online

What you can control, teach, and model



Control

Your biggest influence is what devices your kids access. Remember that they may have access to devices through school, so be aware of what protections the school district implements.

Reality check: Kids can find workarounds to all of the technical safeguards listed here. Settings/controls often change, and age verification is easy to bypass. Think about oversight and controls as speed bumps, not walls for children. And consider loosening controls as kids get older to teach them responsible use.

Technical safeguards

- Parental controls (limit content, contacts, chats, purchases)
- Set screen time limits (limit how long kids can spend on smartphones, tablets, or games)
- Safe search settings (limit explicit, mature, or graphic content on browsers)
- App permissions (limit what information apps can access: location, photos, contacts, camera/mic)
- Privacy settings on accounts/profiles (limit who can see content on a user's profile)
- Home Wi-Fi Settings (limit content and how long users can access the internet)

Implementing Technical Safeguards	
Where to look	Built-in settings like "Screen Time" (Apple), "Digital Wellbeing" / "Family Link" (Android), or within the specific app, game, console, or router itself.
Can't find it?	Search "[device or app name] + screen time limits" (or "parental controls," "safe search," etc.). Companies publish their own guides; ConnectSafely, Internet Matters, and Common Sense Media post tutorials.
Check every device	Check all devices, apps, and browsers. Don't forget school issued devices.
Lock it down	Set a PIN or passcode your child doesn't know, so settings can't be changed without you.
Revisit often	Companies change settings and menus, and kids pick up new hacks. Recheck regularly.

Monitoring apps like Bark, Qustodio, and Aura exist and can help caregivers oversee their children's devices. To decide if they are right for your family consider cost, whether it collects/sells data, and if there is a risk of damaging trust with the children that are being monitored.

Teach

Teach about good habits of digital citizenship and create household tech agreements together— shared rules for screen time, contacts, sharing, device use, and passwords.

Common Sense Media: Family Media Agreement; Family Device Agreement; Family Tech Planner

Connect Safely: Family Contracts and Pledges

Internet Matters: Digital Family Agreement

...or search online for many more examples and templates to inspire your own!

Digital citizenship habit	What it means
Treat others well	Words hurt online too. Don't share others' photos or info without consent.
Represent yourself responsibly	Posts are permanent, even if deleted.
Protect privacy	Create strong passwords, maintain private profiles, and keep ID info private. Know grooming red flags: secrecy, requests for photos/info, isolation from friends/family, escalating conversation, threats.
Evaluate what you see	Feeds run on engagement, not accuracy. Ask: Who made this, and why? Can I confirm it elsewhere? What is it trying to make me feel or do?
Know when to ask for help	Confide in a trusted adult when something feels uncomfortable, scary, or suspicious.

The Attention Economy

Teach kids that platforms profit from keeping them scrolling, so infinite scroll, autoplay, and likes/badges are design choices by companies to trigger dopamine and remove natural stopping points. Kids' developing brains are especially vulnerable, with real effects on attention, memory, and sleep. Understanding the design can help kids recognize its harms.

Model

- Be curious (not judgmental) about your child's online life: ask what they're into and who they follow
- Make sure kids know they can come to you with problems and not get punished
- Mind your own posting: ask permission before posting about your kids
- Narrate your own choices ("I'm putting my phone away at dinner because I want to talk to you")