



A Parent's Guide to Keeping Children Safe and Well Online

Apps parents of 11-year-olds should be cautious about or block

- **TikTok, Instagram, Snapchat** – Risk of inappropriate content, adult interactions, and pressure around likes/followers.
- **Ask.fm, Yik Yak** – Anonymous Q&A platforms, often linked to bullying.
- **Kik, Telegram, Discord** – Messaging apps with little moderation, strangers can easily contact kids.
- **Live streaming or friend-matching apps (Bigo, Wink, Yubo)** – Random video chat, exposure to strangers.
- **Hidden vault apps (like "Calculator+")** – Used to hide images or chats from parents.
- **AI companion/chatbot apps (Replika, Character.AI, etc.)** – Can foster manipulative or overly adult conversations.
- **Roblox** – Very popular, but includes user-generated content and in-game chat; needs parental controls enabled.
- **CapCut** – Video editing app linked to TikTok trends; potential exposure to adult content.
- **Wizz (and similar "friend-making" apps)** – Sometimes described as "Tinder for kids," high predator risk.

How parents can monitor app downloads on devices they pay for

On iPhones / iPads (Apple Family Sharing)

1. **Set up Family Sharing** and add your child's Apple ID under your family account.
2. **Enable "Ask to Buy"** – every time your child tries to download an app (free or paid), you get a notification to approve or deny it.
3. In **Settings > Screen Time**, you can also:
 - Restrict apps by age rating.
 - Block "installing apps" altogether unless you allow it.
 - Get weekly reports of app usage.

On Android phones (Google Family Link)

1. Install **Google Family Link** on your phone and your child's device.
2. Link their Google account under your supervision.
3. Turn on **"Require approval for all app downloads"** – you will get a notification each time they request one.
4. Use Family Link to:
 - Block apps by category (social, chat, etc.).
 - Limit screen time per app.
 - View daily, weekly, or monthly app activity reports.

General practices for all devices

- **Keep passwords private:** Don't share the Apple ID or Google Play account password with your child.
- **Regularly review installed apps:** Sit down together weekly to go through what's on the phone.
- **Talk about why rules exist:** Explain safety reasons so it feels like guidance, not just control.
- **Make app use a privilege, not a right:** Clear consequences if rules aren't followed.

