

Online Safety News

DECEMBER 2025



Staying Safe Over the Holidays

If new devices, games or apps come into your house this month, it's important to take some time to get ahead. **Setting things up properly from day one is one of the simplest ways you can protect your child.**

Here's what really matters:



1. Turn on the highest privacy settings available

Most apps start on the lowest privacy setting, which means children's profiles, photos or gameplay can be visible to anyone. Switch everything to private before they start using it – not after.

2. Check who they can talk to

Games like Fortnite, Roblox and Minecraft, plus apps like Instagram, Snapchat and TikTok, all have voice, chat or DM functions. These are often the biggest risk points. Make sure chat is off, friends-only or supervised.

3. Turn off location sharing



Many platforms quietly track location by default. Kids don't need strangers seeing where they live, where they go to school or when they're online.

4. Set age-appropriate filters



On games and social apps, filters reduce violent, sexual or adult content. Even with filters on, nothing is perfect – but it's a huge improvement on having no boundaries at all.


5. Switch on spending controls

Whether it's V-Bucks, Robux, skins or upgrades, in-game spending can spiral quickly. Put passcodes or parental approvals in place so you stay in control, not the game.

6. Talk before they tap



No setting replaces conversations. Ask your child what they want to use, why, what they think the risks could be and who they think it's safe to talk to online. Children are far more likely to come to you if something goes wrong when they feel included, not monitored.



Internet Matters have a full breakdown parental controls and how to set them up on any device, game or app. You can find this here: [Parental controls and privacy settings guides | Internet Matters](#)

Telegram: Is It Safe? Rated 16+



Telegram

Telegram might look like “just another messaging app,” but it’s one of the riskier platforms children and teens can use — and it’s important we know why.

Telegram is designed for **anonymity**, **huge unmoderated groups**, and **private channels** where anything can be shared with no real oversight. That combination makes it a hotspot for strangers, explicit content, scams, and people who actively seek out children and teens.

The biggest risks for young people:



- **Strangers can contact them easily**, even without knowing their phone number.
- **Adult and explicit content** is common in public groups and channels — and there are no meaningful filters.
- **Anonymous usernames** mean kids have no idea who they’re actually talking to.
- **Extremist, violent, or illegal content** appears more often on Telegram than on most mainstream apps.
- **Group-chats can include thousands of unknown people**, making children extremely visible and vulnerable.



For younger children, Telegram is simply **not appropriate**. For teens, it needs **active supervision**, **clear boundaries** and **very limited use**. Disable the “add to group” setting, avoid all public groups/channels, and encourage sticking to real-life contacts only.



Safer Search Engines for Kids: Swiggle & Kiddle

If your child is starting to explore the internet on their own, two great options to keep things safer are **Swiggle** and **Kiddle**.



They work just like Google, but with strong filters that block adult content, reduce inappropriate results and guide children towards age-appropriate websites. They’re not perfect — nothing online ever is — but they’re a far better first step for younger users who are curious and still learning how to search safely. Adding Swiggle or Kiddle as the default search engine on your child’s device gives them the freedom to explore, while giving you peace of mind that they’re less likely to stumble across something they’re not ready for.