10 things every family can do at home

Protecting children from online grooming and harmful AI influence

01 Set accounts to private.

Review every game, social app, and messaging service together. Check who can see posts, send messages, or add your child to groups.[1]

02 Check every chat route.

Review voice chat, direct messages, invitations, and friend lists. Restrict unapproved contacts. Use the platform checklist on page 3.[1]

03 Keep personal details private.

Teach children not to share their school, address, phone number, location, or personal photos with people they only know online.[1]

04 Set a rule about meetups.

No meeting an online-only contact without a parent involved and present. Someone who feels familiar online may not be who they claim.[1]

05 Notice pressure and secrecy.

Discuss gifts with strings attached, requests for images, and pressure to switch apps or keep secrets. Grooming can look like trust-building.[2]

06 Make disclosure feel safe.

Say, “You can come to me, even if you broke a rule.” Listen calmly, address safety first, and reinforce that abuse is not their fault.[2]

07 Keep AI tools in their place.

Our recommendation: no AI companions for minors. Distinguish learning tools from friends, partners, or therapy; keep trusted people central.[3]

08 Ask how your child uses AI.

Review use together. Ask what they figured out independently, where they disagreed with an answer, and how they checked it.[4]

09 Verify before sharing.

AI can fabricate realistic images and videos. Check who posted it, seek reliable evidence, and ask what it wants you to believe or do.[5]

10 Make time for conversation.

Build regular check-ins at meals, in the car, or after school. Stay curious and calm. Make it easy to ask for help.

Start with one change tonight. These steps cannot guarantee safety. Abuse is the offender's responsibility, never the child's.

Sources

1. Internet Matters: https://www.internetmatters.org/issues/online-grooming/protect-your-child/
2. NSPCC: https://learning.nspcc.org.uk/safeguarding-child-protection/grooming
3. AACAP: https://www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/AI_Chatbots-148.aspx
4. Common Sense Media: https://www.commonsensemedia.org/articles/ai-chatbots-and-your-child-age-and-stage-guidance
5. DHS Know2Protect: https://www.dhs.gov/sites/default/files/2025-07/25_0801_k2p_p2p_AI-Deepfakes.pdf

Age rules first. Readiness next.

Meet each service's current age rules. An eligible age does not establish readiness; this is a recommended household framework, not a list of legal minimums.[1]

5 and younger	Adult-managed, age-appropriate experiences. No open stranger chat; use devices with an adult present. **AI:** No chatbots.[2]
6 to 8	Adult-managed access. Allow communication only with family or approved contacts; keep unapproved chat off. **AI:** Limited adult-accompanied use, only where the service permits it.[2]
9 to 12	Use child-appropriate services and approved contacts. Review friends and servers together; approve new apps. **AI:** Limited adult-accompanied use where permitted; no age-rule workarounds.[2]
13 to 15	Introduce eligible services gradually. Review messaging, location, communities, and contacts separately. **AI:** Supervised learning or creative tasks, not companionship.[2]
16 to 17	Increase independence based on skills and behavior. Keep agreed check-ins and make sure teens can block, report, and seek help. **AI:** Learning and creative use with accountability; not emotional or mental-health support.[2]

Sources

1. American Academy of Pediatrics: https://www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/qa-portal/qa-portal-library/qa-portal-library-questions/age-to-introduce-social-media/

2. Common Sense Media: https://www.commonsensemedia.org/articles/ai-chatbots-and-your-child-age-and-stage-guidance

Check the settings, together.

Use the child's account. Settings vary by age, region, account, and version.

☐ **Roblox**	Review Parental Controls > Communication; use No one for unapproved chat. Developer-created chat is not covered.[1]
☐ **Minecraft / Xbox**	Set voice, text, and invitations to Friends or Block; review multiplayer and friend permissions.[2]
☐ **Fortnite / Epic**	Review voice/text chat and PIN-protect Epic friend requests; check console controls separately.[3]
☐ **Discord**	Connect Family Center; review contacts, servers, and filters. It does not show message contents.[4]
☐ **YouTube**	Use a supervised pre-teen experience for younger children; review content limits and communication restrictions.[5]
☐ **TikTok**	Use Family Pairing; review privacy, comments, reuse, and messages. Direct messages require age 16+.[6]
☐ **WhatsApp**	Run Privacy Checkup: limit groups and visibility; silence unknown callers. Unknown messages may still arrive.[7]
☐ **Kik**	If permitted, keep usernames and Kik Codes private; review New Chats. Group members can see usernames.[8]
☐ **Snapchat**	Enable Ghost Mode. Snaps submitted to Snap Map can still appear there; review location sharing separately.[9]
☐ **Instagram**	Keep stricter teen message settings; review approved connections that can enable messages.[10]
☐ **Facebook / Messenger**	Review teen messaging, friends, and phone contacts, not just profile visibility.[10]
☐ **X**	Enable Privacy and safety > Audience and tagging > Protect your posts; this controls post visibility.[11]

Sources

1. Roblox: https://en.help.roblox.com/hc/en-us/articles/30428310121620-Parental-Controls-Overview
2. Minecraft: https://www.minecraft.net/en-us/article/parental-controls
3. Epic Games: https://safety.epicgames.com/parental-controls
4. Discord: https://support.discord.com/hc/en-us/articles/14155043715735-Family-Center-for-Parents-and-Guardians
5. YouTube: https://support.google.com/youtubekids/answer/10314940?hl=en-GB
6. TikTok: https://support.tiktok.com/en/safety-hc/account-and-user-safety/family-pairing
7. WhatsApp: https://faq.whatsapp.com/143990998547188
8. Kik: https://help.kik.com/hc/en-us/articles/4402351911835-Keep-your-Kik-account-private
9. Snapchat: https://help.snapchat.com/hc/en-us/articles/7012322854932-How-do-I-turn-on-Ghost-Mode
10. Meta: https://about.fb.com/news/2024/01/introducing-stricter-message-settings-for-teens-on-instagram-and-facebook/
11. X: https://help.x.com/en/safety-and-security/how-to-make-x-private-and-public

Safety first. Stay calm.

“You can come to me.
We will work through this together.”

Listen without blame.

If a child discloses abuse, listen and reassure them that it is not their fault.[1]

Preserve the original communications.

Do not delete messages or forward sexual images of a child to another device. Contact law enforcement; DHS advises considering airplane mode with Wi-Fi and Bluetooth off to protect evidence from remote alteration.[2]

Use the right reporting route.

In the U.S., report suspected child sexual exploitation through NCMEC’s CyberTipline, or call DHS Know2Protect at 833-591-5669. Call 911 for an immediate emergency.[2,3] Elsewhere, use local emergency or child-protection services.

Your next family check-in

Choose one platform, make one settings change, and practice one safety conversation. Set a date to review again.

Platform: _____ Next review: _____

Sources

1. NSPCC: https://learning.nspcc.org.uk/safeguarding-child-protection/grooming
2. DHS Know2Protect: https://www.dhs.gov/sites/default/files/2025-07/25_0801_k2p_p2p_AI-Deepfakes.pdf
3. NCMEC CyberTipline: https://www.missingkids.org/gethelpnow/cybertipline