



SOCIAL MEDIA

Teen Social Media Safety Checklist

Platform-by-platform privacy settings guide

Instagram, Snapchat, Telegram, Discord, TikTok, and more — what to lock down, what to watch for, and how to have the conversation without shutting your teen down.

PLATFORM RISK AT A GLANCE

MANAGEABLE**Instagram**

Now has a dedicated "Teen Accounts" mode with built-in restrictions. Lockable with parental supervision. See Step 1.

HIGH RISK**Snapchat**

Messages disappear by design — creating cover for sexual exploitation and bullying that leaves no trace. Snap Map broadcasts real-time location. Among platforms most cited in sextortion and CSAM cases. Family Center has limited visibility. See Step 5.

HIGH RISK**Telegram**

No parental controls. Secret chats are end-to-end encrypted and auto-delete. Frequently used to share explicit content and coordinate predatory behavior. Not appropriate for teens.

CAUTION**Discord**

Popular for gaming but contains adult-only servers teens can access. No robust parental controls. Requires active monitoring of which servers they're in. See Step 6.

HIGH RISK**BeReal / Yubo**

Yubo is designed as a "live social network" for teens but is frequently associated with predatory contact. No parental controls. BeReal has location metadata risks.

CAUTION**TikTok**

Has Family Pairing for parental controls. Algorithm can accelerate harmful content quickly. Private accounts don't prevent DMs from strangers by default. See Step 7.

1

Set up Instagram parental supervision and lock Teen Account settings

On your teen's Instagram, go to Settings & Activity → Supervision → Invite supervisor. Accept from your own account. Once linked, open Instagram on your phone → Settings → Supervision → select your teen. Turn on "Require supervisor approval to change settings" so they can't disable restrictions without your approval. Confirm their account is set to Private and that DMs are restricted to followers only.

2

Turn on "Sensitive Content Control" and enable hidden words

In Instagram supervision settings, set Sensitive Content Control to "Limit Even More." Then go to your teen's Settings → Hidden Words → turn on "Hide comments" and "Hide DM requests" for offensive words. Also turn on "Advanced comment filtering." This won't catch everything but significantly reduces exposure to hate speech, eating disorder content, and explicit material.

3

Set a daily time limit and enable "Take a Break" reminders

In your supervision dashboard, go to Time → set a daily time limit (most child psychologists recommend 60-90 minutes for teens). Enable "Take a Break" reminders every 20-30 minutes. You can also set "Bedtime Mode" which mutes notifications and shows a reminder at a set time — set it to 9:30 PM on school nights.

RED-FLAG APPS — WHAT TO DO



SOCIAL MEDIA

Teen Social Media Safety Checklist

Platform-by-platform privacy settings guide

4

Have a direct conversation about Telegram — then check if it's installed

Telegram is not appropriate for teens. It has no age verification, no parental controls, and "secret chats" are end-to-end encrypted with auto-delete by design — creating a communication channel with zero visibility. Telegram has been directly implicated in the distribution of CSAM (child sexual abuse material) and in coordinating sextortion campaigns targeting minors. Don't ban it silently — have the conversation. Check their phone for it (iOS: search "Telegram" in Spotlight; Android: Settings → Apps). If found, remove it together, not unilaterally.

5

Understand the real Snapchat risk — set up Family Center, disable Snap Map, and have the sextortion conversation

Why Snapchat is now High Risk: Snaps disappear by design — which is exactly what predators rely on. Sextortion on Snapchat works like this: a stranger (posing as a peer) befriends your teen, builds trust, asks for a photo, then immediately threatens to share it unless paid or given more. Because messages vanish, teens often feel they have no proof and no recourse. They don't tell parents because they're ashamed. This pattern has led to teen suicides. Bullying via Snapchat is also uniquely hard to document — the evidence deletes itself. Setup steps: In Snapchat, go to your teen's profile → Settings → Family Center → Invite parent. Accept from your Snapchat to link. Family Center shows friend lists and content exposure categories — not message content. Go to Snap Map → settings gear → set to "Ghost Mode." Also go to Settings → Privacy Controls → set "Who Can Contact Me" to "Friends Only" and "Who Can See My Story" to "Friends Only."

6

Audit which Discord servers your teen is in

Ask your teen to show you their Discord server list — treat it like checking which clubs they joined at school. Age-restricted servers (18+) require age verification but teens easily lie about their age. Red flags: servers with adult-only tags, invite-only servers with no context, or servers with very large numbers of strangers. Enable "Safe Direct Messaging" in Discord settings → Privacy & Safety → set to "Filter all direct messages." Turn off "Allow direct messages from server members" on any server where they don't personally know everyone.

TIKTOK

7

Enable TikTok Family Pairing and set DM restrictions

On TikTok, go to your teen's profile → Settings → Family Pairing → Teen. Scan the QR code with your TikTok (or create one) to link accounts. In your Family Pairing dashboard, set: Screen Time Limit (recommended: 60–90 min/day), Restricted Mode ON, Direct Messages OFF or limited to "Friends only." By default, TikTok accounts under 16 cannot send or receive DMs — confirm this is still the case and hasn't been bypassed.

CROSS-PLATFORM RULES

8

Set all accounts to private — and verify it stuck

Instagram, TikTok, Snapchat, and most platforms have a "Private Account" toggle. Go through each one and confirm it's on. Then verify: log out of the app, search your teen's username — if you can see their posts without following, it's not actually private. Some apps (like TikTok) require separate settings for profile visibility vs. content visibility.



SOCIAL MEDIA

Teen Social Media Safety Checklist

Platform-by-platform privacy settings guide

9

Disable "Allow others to find me by phone number or email"

Every major platform has this setting — it lets anyone who has your teen's phone number add them or find their profile. Turn it OFF on: Instagram (Settings → Account → Contact Syncing), TikTok (Settings → Privacy → Suggest your account to others), Snapchat (Settings → See Me in Quick Add), Discord (Settings → Privacy & Safety → "Let others find me" options). This one setting closes a common vector for stranger contact.

10

Do a "stranger DM" check — and set the rule

Look through your teen's DM requests or message requests folder on Instagram, Snapchat, and TikTok. You will almost always find stranger messages. Use this as a teaching moment, not a gotcha. Research consistently shows teens respond better to clear rules with reasons than to monitoring-only approaches — and to parents who stay curious rather than reactive.

THE CONVERSATION

11

Establish three rules — together — and write them down

The research on teen online safety is clear: teens who feel trusted and heard are more likely to come to parents when something goes wrong. Set three household rules together (not imposed): (1) Never share personal info — real name, school, address, phone number — with anyone you only know online. (2) If someone makes you uncomfortable or asks for photos, tell a parent immediately, no judgment, no consequences for coming forward. (3) No new apps without checking in first. Write these on a card. Review together every 3 months — their digital life changes fast.