

 PARENT TOOLKIT

Back-to-School Digital Setup: The 30-Minute Family Tech Reset

By the DSK Research Team · August 2026

A new school year means new devices, new apps, new class group chats, and often a new phone. It's the single best moment all year to reset your family's digital safety setup together — before habits (and privacy settings) drift for another year. This issue is deliberately practical: one sitting, about 30 minutes, done together with your child.

30 Minutes

once a year, done together, catches more preventable risk than months of after-the-fact monitoring. Treat it like a fire drill: brief, routine, no drama.

Step 1 — Privacy Settings Audit (8 minutes)

Sit with your child and go through every app on their phone together. Set social accounts to private. Set game chat to "friends only" rather than "everyone." Turn off precise location sharing on apps that don't need it for anything functional. Doing this together — rather than for them — means they understand why each setting matters, not just that it changed.

Step 2 — Platform-Specific Protections (8 minutes)

- **Roblox:** enable Account Restrictions in settings; confirm chat is set to friends-only (see our Roblox Parent Guide for exact steps).
- **Instagram / TikTok:** set the account to private; turn off ad personalization; disable autoplay if the option exists.
- **New school-issued devices:** ask the school directly what monitoring or filtering software is installed, and what it does and doesn't cover — many parents assume more coverage than actually exists.
- **New group chats:** a new class or team almost always means a new group chat within the first week. Ask who's in it, and whether it's monitored by an adult.

Step 3 — The Family Media Agreement (8 minutes)

Rather than a one-sided rule list, write a short agreement together — what hours are phone-free, whether phones charge outside the bedroom overnight, and what happens if something online goes wrong. A rule your child helped write is dramatically more likely to be followed than one handed down.

DON'T SKIP THIS PART

Refresh your family code word this year — a word only your family knows, used to verify identity if anyone calls or messages claiming to be a relative in an emergency. Voice-cloning scams targeting families are common enough that this five-minute step belongs in every year's reset.

Step 4 — Save the Emergency Numbers (3 minutes)

Add NCMEC's CyberTipline and DSK's emergency resources directly into your child's phone contacts before they need them, not after. In a moment of panic, a saved contact gets used; a website they'd have to search for often doesn't.

"The families who handle a digital safety incident well aren't the ones with the most restrictive rules — they're the ones who did the boring setup work in a calm moment, months before anything went wrong." — DSK Research Team

Quick Action Checklist

- ☐ Privacy settings reviewed on every app, together
- ☐ Roblox Account Restrictions + friends-only chat enabled
- ☐ Asked the school what monitoring exists on issued devices
- ☐ New class/team group chats identified and reviewed
- ☐ Family media agreement written together for the new year
- ☐ Family code word refreshed
- ☐ Emergency numbers saved directly into your child's phone

THE MOST IMPORTANT THING YOU CAN DO

Make this an annual ritual, not a one-time lecture — same week every August, same 30 minutes, done together. Consistency is what makes it stick, not thoroughness in any single year.

Resources

- DSK Roblox Parent Guide, Family Cybersecurity Checklist — both at digitalsafetyknights.org (Guides section)
- DSK Family Safety Audit: digitalsafetyknights.org/audit.html

- DSK Emergency Help: digitalsafetyknights.org