

Parent's Guide to Digital Safety

Practical Strategies for Managing Screen Time, Social Media & Gaming (Ages 6–18)

Golden Rule: No Devices in Bedrooms & Overnight

All phones, tablets, and gaming consoles should be collected at a central charging station outside bedrooms at least **60 minutes before bedtime**. Sleep disruptions caused by late-night notifications, blue light exposure, and unmonitored night usage severely impact brain development, mood regulation, and academic performance.

AGE-BASED SCREEN TIME & USAGE RECOMMENDATIONS

Screen time recommendations focus on balancing digital engagement with real-world physical health, academics, and sleep.

Age Group	Daily Limit (Non-Academic)	Recommended Boundaries & Focus
Ages 6–9	1 Hour / Day	High parent co-viewing. Content should be purely educational or creative. No personal social media accounts or online multiplayer chat.
Ages 10–12	1.5 Hours / Day	Introductory moderated gaming. Parental controls active. Social media still strongly discouraged or limited to family-only channels with strict monitoring.
Ages 13–15	2 Hours / Day	First introduction to social media with private profiles. Clear rules on privacy settings and friend lists. No devices during homework hours or meals.
Ages 16–18	2.5–3 Hours / Day	Focus on digital self-regulation and time management before adulthood. Open conversations regarding digital footprint, online reputation, and mental health.

ESSENTIAL GAMING SAFETY GUIDELINES

Online Interaction & Privacy

- Disable public voice and text chat in multiplayer games for children under 13.
- Teach children never to reveal their full name, school, city, or phone number.
- Ensure gamer tags and avatars are anonymous and contain no personal identifiers.

In-Game Purchases & Microtransactions

- Keep credit cards disconnected from console and app store accounts.
- Enable password authentication for every purchase or transaction.
- Educate kids on loot boxes, gambling mechanics, and predatory purchasing incentives.

Parent Check-In Action Item

Check the ESRB rating (e.g., E, E10+, T, M) before allowing any game download. Pay close attention to interactive elements like "In-Game Purchases" or "Users Interact".

SOCIAL MEDIA SAFEGUARDS & HEALTHY HABITS

Social platforms are designed to maximize engagement. Use these practices to protect emotional well-being and privacy.

Account Security & Privacy

- Set all accounts to **Private** by default.
- Regularly review follower/friend lists together to audit unknown contacts.
- Turn off precise location permissions (geotagging) in camera and social media apps.

Mental Health & Well-being

- Discuss the reality of curated online personas versus real life.
- Establish tech-free zones (e.g., dining table, family rooms, cars).
- Encourage immediate reporting of cyberbullying or feeling uncomfortable without fear of device revocation.

EMERGING THREATS: AI, DEEPPAKES & IMAGE MANIPULATION

Artificial intelligence tools now make it easy to manipulate photos, clone voices, or create realistic synthetic media.

Best Practices for AI Tools

- Teach kids never to enter personal information, home addresses, or private photos into AI chatbots or image generators.
- Treat AI output as unverified—always double-check facts and sources before trusting generated information.
- Set clear boundaries on using generative AI for schoolwork to maintain academic integrity.

Navigating Deepfakes & Edited Photos

- **Limit Public Photos:** Keep social media accounts private to prevent public photos from being scraped for AI cloning.
- **Verify Unusual Media:** Teach children that manipulated images or audio can be used for bullying or fake emergency scams.
- **Reporting Protocol:** If an explicit or harmful deepfake is created of a child, report it immediately to school authorities, the hosting platform, and law enforcement.

Protecting Photos Online

Emphasize to teens that once a photo is posted or sent online, control over that image is lost permanently. Discourage posting high-resolution personal photos on public forums.

PLATFORM PARENTAL CONTROLS GUIDE

Most major social and gaming platforms offer built-in parental supervision hubs. Here is how to configure safety settings on popular platforms.

TIKTOK

Family Pairing

Links a parent's account to their teen's account to manage settings remotely.

- **How to Set Up:** Open TikTok on your device > Profile > Menu (3 lines) > Settings & Privacy > **Family Pairing**. Select *Parent* and scan the QR code generated on your teen's phone.
- **Key Features:** Set daily screen time limits, block search keywords, disable direct messaging, and turn on Restricted Mode to filter mature content.

SNAPCHAT

Family Center

Offers insight into interactions without revealing private chat contents.

- **How to Set Up:** Open Snapchat > Profile Icon > Settings (Gear) > Privacy Controls > **Family Center**. Send an invitation link to your teen to accept.
- **Key Features:** View friend list, see who they chatted with in the past 7 days, turn on *Hide Sensitive Content* in Stories/Spotlight, and request location check-ins.

DISCORD

Family Center

Monitors gaming server communities and direct messaging activity.

- **How to Set Up:** Teen opens Discord > User Settings > **Family Center** > Generate QR Code. Parent opens Discord mobile app > Settings > Family Center and scans teen's code.
- **Key Features:** View recently added friends, server activity, weekly activity summary emails, sensitive media filters, and setup spending caps or downtime.

INSTAGRAM

Parental Supervision

Built-in Family Center tools to manage screen time and contacts.

- **How to Set Up:** Open Instagram > Profile > Menu (3 lines) > Settings > **Supervision**. Create an invite link and send it to your teen to connect.
- **Key Features:** Manage daily limits, schedule mandatory breaks, review accounts they follow/are followed by, and restrict DMs to contacts only.

GAMING CONSOLES (ROBLOX, NINTENDO SWITCH, PLAYSTATION, XBOX)

Console & Game Safety Hubs

- **Roblox:** Go to Settings > Parental Controls. Link a parent email, enable a 4-digit Account PIN, and set age-based Content Maturity Ratings to restrict unrated experiences.
- **Nintendo Switch / Xbox / PlayStation:** Download their dedicated parent apps (e.g., *Nintendo Switch Parental Controls app*, *Xbox Family Settings app*) to enforce strict play-time limits, block voice chat, and restrict online store purchases with a PIN.

FINANCIAL SEXTORTION: PREVENTION & RESPONSE

Financial sextortion is a dangerous crime targeting teenagers (especially young men) on social media, direct messaging, and gaming apps.

How Sextortion Scams Work

Perpetrators create fake online profiles (often posing as an attractive peer) to cultivate trust. They quickly pressure the victim to send explicit images or move to a secondary messaging app, then immediately demand money or gift cards under threat of sharing the image with family, friends, or schools.

Prevention Strategies

- **Be Wary of Rapid Intimacy:** Warn kids about unknown followers who quickly compliment them or demand private photo exchanges.
- **Strict Privacy:** Keep follower lists hidden so scammers cannot leverage threat lists of friends/family.
- **Open Communication:** Reassure your child that if they fall victim, they are not in trouble and should seek help immediately.

Immediate Steps if Targeted

- **DO NOT PAY:** Paying money rarely stops the demands and often leads to higher extortion requests.
- **Stop Communication:** Do not reply to threats, but do not delete the account or conversation.
- **Save Evidence:** Take screenshots of the profile, chat history, handle, and payment details.
- **Report Immediately:** Report to the platform, local police, and NCMEC at [TakeltDown.ncmec.org](https://www.takeldown.ncmec.org) or 1-800-843-5678.

FAMILY TECH AGREEMENT BLUEPRINT

A proactive agreement reduces arguments by setting clear, transparent expectations around digital devices.

Core Family Commitments

- **Overnight Protocol:** All phones, tablets, and controllers must be in the central station by 8:00 PM (for under 13) or 9:00 PM (14+).
- **Transparency Rule:** Parents have access to passcodes and will perform periodic, non-punitive safety check-ins.
- **Digital Footprint Standard:** Nothing gets posted or shared that couldn't be shown to a grandparent, teacher, or future employer.
- **No-Blame Support:** If a safety issue or threat arises (such as harassment or extortion), kids can report it without losing device privileges.

Final Thought for Parents

Model the behavior you wish to see. Children copy adult screen habits—keep family time tech-free and demonstrate intentional phone use.