PRESENT AGE
MINISTRIES

A Parent's Guide to Parental Controls

Devices • Apps • Software | Practical choices for safer digital experiences | Updated October 2026

Start with connection—not just restrictions

No parental control can prevent every risk, read every message, or replace a trusted adult. Explain what you monitor and why, invite questions without shame, and make a plan for what your child should do if something uncomfortable happens online.

Three layers of protection

1 Built-in controls (often free). Manage screen time, downloads, purchases, privacy and content restrictions directly through a device or account.

2 Additional software (often paid). Add filtering, activity reports or alerts. Features vary considerably by device, browser and app.

3 Child-focused devices and home networks. Consider simplified phones or watches and router-level filtering for shared household devices.

A practical starting checklist

☐ Create a child account with the correct birth date; connect it to a parent-managed family group.

☐ Require approval for new apps and purchases; review installed apps regularly.

☐ Set age-appropriate content filters, privacy controls, and limits on who can contact your child.

☐ Turn off unnecessary location sharing; review camera, microphone and contact permissions.

☐ Set screen-free routines, especially at bedtime; keep software updated.

☐ Agree on a no-punishment-first response when a child reports threats, explicit content or unwanted contact.

1 | Free controls built into devices

Apple Screen Time + Family Sharing — iPhone, iPad, Mac. Set app and website access, usage schedules, communication restrictions and purchase approvals. Newer software versions add additional family safety options; availability depends on software version and device. Start: Settings → Family → child → Screen Time. apple.com/families

Google Family Link — Android and Chromebook. Manage compatible supervised devices, app approvals, time limits, location and Google content settings. A parent may manage from an iPhone, but Family Link does not supervise a child's iPhone or iPad. families.google/familylink

Microsoft Family Safety — Windows and Xbox. Manage screen time, games and app limits, plus web filters when using Microsoft Edge. Some features differ by platform. microsoft.com/microsoft-365/family-safety

Gaming and entertainment accounts. Set separate parental controls inside Roblox, Xbox, PlayStation, Nintendo, YouTube and streaming services. Console or device controls may not cover chats, user-generated content or every third-party service.

What these controls may NOT do

A device limit does not necessarily inspect messages, stop a child from using a different device, or prevent harmful interactions in an approved game. Revisit settings after major operating-system or app updates.

Questions to ask before choosing a tool

Which devices does my child actually use? Do I need limits, content filtering, risky-content alerts, location tools, or all four? Can my child use the same account on a school device or friend's phone? What information does the service collect and who can access it?

2 | Additional software and monitoring

Bark — monitoring and alerts. Offers alerts for potential concerns, filtering, schedules and location tools. Monitoring coverage differs between Android and iPhone; iPhone monitoring can require extra setup and supported account connections. bark.us

Qustodio — time management and filtering. Offers web/app filtering, schedules, activity reports and selected communication monitoring. Coverage and setup vary by operating system and feature. qustodio.com

Circle — home and device internet management. Focuses on filtering, internet time limits and household routines. Check whether the desired protection applies away from home Wi-Fi and to cellular connections. meetcircle.com

Compare by need—not brand name

Time limits and app approvals – Start with Apple Screen Time, Google Family Link or Microsoft Family Safety.

Risk alerts across supported messages – Consider monitoring software; confirm exactly which apps and devices it can inspect.

Home Wi-Fi limits and filtering – Consider router or network-level controls; these may not apply on cellular data.

More restricted first device – Consider a child-focused phone or watch with limited apps and contacts.

Paid services are examples, not endorsements. Prices, compatibility, coverage and policies change; confirm current details before purchasing.

Privacy and trust matter

Tell children what will be monitored in age-appropriate language. Choose the least intrusive tool that meets the safety need. Protect parent passwords, enable multifactor authentication and avoid sharing sensitive screenshots or messages unnecessarily.

3 | Devices and home protection

Child-focused phones — e.g., Bark Phone or similar. Designed to offer stronger parent management of apps, contacts and device settings. Compare carrier requirements, monthly fees, emergency calling, accessibility and whether restrictions can be changed as your child matures.

Connected watches — e.g., child-oriented GPS/calling watches. Can provide location and limited communication without a full social-media phone. Review approved-contact controls, location accuracy, battery life and emergency features.

Home routers / network filters. Can limit sites or internet access for connected household devices. They may not cover mobile data, encrypted traffic or devices connected elsewhere.

A simple family technology agreement

☐ We will review new apps and online contacts together.

☐ We will not share passwords, intimate images, addresses or live location with online strangers.

☐ We will tell a trusted adult about secrecy demands, threats, requests for sexual images, or pressure to meet.

☐ If someone threatens to share an image, we will not pay or send more images; we will get help.

☐ We will revisit rules together as maturity, needs and technology change.

If something concerning happens

Stay calm and listen. Do not blame or punish a child for disclosing. If there is immediate danger, call 911. Preserve relevant usernames, links and messages where safe, but do not download, forward or circulate sexual images of minors. Report suspected online child sexual exploitation to NCMEC's CyberTipline at report.cybertip.org or 1-800-THE-LOST (1-800-843-5678).

Learn more

Product and setup references: support.apple.com/en-us/108806 ◦ families.google.com/familylink ◦ microsoft.com/en-us/microsoft-365/family-safety ◦ bark.us ◦ qustodio.com

Educational information only. Features are subject to change; confirm current settings and compatibility with each provider.