

Protecting child online privacy



Why child online privacy matters

Child online privacy is the protection of a child's personal information, identity, communications, location, images, behavioral data, and digital reputation. It matters because childhood is a period of rapid neurodevelopment, social learning, and identity formation. A child may enjoy an app or game in the moment without understanding how a username, birth date, photo, device identifier, browsing pattern, or voice recording could be stored, analyzed, shared with third parties, or used to influence what they see next.

Privacy is also a health-adjacent issue. Loss of privacy can contribute to stress, embarrassment, social exclusion, bullying, coercion, or fear of being watched. Adolescents, in particular, may experience intense shame or anxiety when private images, messages, or mistakes are circulated. This does not mean every online activity is harmful; digital spaces can support learning, creativity, disability access, social connection, and peer belonging. The aim is to preserve these benefits while reducing preventable exposure.

Research reviews suggest that children's understanding of privacy is uneven. Many children grasp interpersonal privacy, such as not sharing a secret with classmates, earlier than institutional or commercial privacy, such as how a

platform tracks behavior or builds profiles. This gap means adults have an important scaffolding role. Online safety for children is strongest when privacy is treated like seatbelts or bike helmets: a normal protective routine, not a punishment.

What counts as a child's personal information online

Personal information is broader than many families realize. It includes obvious identifiers, such as a child's name, address, phone number, email address, school, photograph, voice, and video. It can also include persistent identifiers that recognize a user over time, such as cookies, device IDs, advertising IDs, IP addresses, and account numbers. Location information, biometric data, contact lists, chat logs, in-app purchases, learning records, and behavioral patterns can also be sensitive.

Children's data may be collected in many settings: educational technology platforms, video-sharing services, social media, multiplayer games, fitness trackers, smart speakers, connected toys, messaging apps, and websites with quizzes or contests. Some collection is necessary for a service to function. For example, a learning platform may need login credentials and progress data. The concern is excessive collection, unclear sharing, weak security, manipulative design, or reuse of information in ways children and parents would not reasonably expect.

Families should also consider the digital footprint created by adults. Posting a child's full name, date of birth, school uniform, medical story, location-tagged photos, or behavioral challenges can create an enduring record before the child can consent. Medically literate readers may recognize the ethical parallel with confidentiality: information about a child's health, neurodevelopment, mental health, or disability deserves careful handling even when the intention is advocacy or community support.

Children's understanding changes with development

A preschool child may follow a simple rule, such as "ask before tapping yes," but cannot evaluate a privacy policy. A school-age child may understand that some information is private, yet still be drawn to rewards, avatars, streaks, or peer approval. Adolescents often want independence and may be highly skilled

with devices, but that technical fluency does not guarantee mature risk assessment. Executive functions, including inhibition, future planning, and emotional regulation, continue developing into young adulthood.

This developmental reality supports graduated responsibility. Younger children benefit from co-use, restricted profiles, carefully chosen apps, and parent-managed privacy settings for child accounts. Older children and adolescents benefit from collaborative review: "Let's look at what this app can access," "Who can see your posts?" and "What would you do if someone asked for a private photo?" The goal is to move from external control toward internal judgment.

Privacy education should not rely on fear alone. If children believe they will be punished for any mistake, they may hide problems. A protective family culture says: "You can come to me if something feels wrong, even if you clicked, shared, or replied." This is particularly important when privacy concerns intersect with cyberbullying and child wellbeing, image-based abuse, grooming, extortion, or threats. In these situations, preserving evidence and seeking adult help is usually safer than deleting everything immediately.

Legal protections and parental rights

In the United States, the Children's Online Privacy Protection Act Rule, commonly called COPPA, applies to operators of websites and online services directed to children under 13, and to services that knowingly collect personal information from children under 13. The rule generally requires clear notice to parents and verifiable parental consent before collecting, using, or disclosing a child's personal information, with limited exceptions.

Parents have rights under COPPA, including the ability to review personal information collected from their child, request deletion, and refuse further collection or use. Services covered by the rule must explain their information practices, including what data they collect, how they use it, and whether they disclose it. If a site or app asks for more information than seems necessary, or makes participation conditional on excessive data collection, that is a reason to pause and investigate.

Legal protections differ by country and may differ for schools, health-related

apps, and educational platforms. Even strong laws cannot replace day-to-day privacy habits because many popular services are designed for older users, and children may misstate their age to access them. Families can support compliance by using accurate birth dates for child accounts, choosing child-appropriate services, and avoiding workarounds that place a child into adult data environments with adult defaults.

Practical privacy habits for families

Privacy protection becomes easier when it is routine. Start with account creation. Use a parent email when appropriate, avoid usernames that include a child's full name or birth year, and provide only the minimum required information. Review default settings because many services favor sharing, discoverability, personalization, or location access unless a user changes them.

Check app permissions before installation and periodically afterward. Ask whether the app truly needs the camera, microphone, contacts, Bluetooth, or precise location.

Turn off public profiles, searchable accounts, location tagging, and friend suggestions when they are not needed.

Use strong, unique passwords and consider a reputable password manager for family accounts.

Enable multifactor authentication for parent-controlled accounts, school portals, and platforms that store photos, messages, or payment data.

Walk through sign-up forms with children so they learn why some questions are unnecessary or risky.

Teach children not to share full names, addresses, school names, schedules, passwords, private images, or one-time verification codes.

It is also worth reviewing connected devices in the home. Smart speakers, tablets, gaming consoles, watches, and toys may collect voice, location, usage, or contact data. Disable features that are not needed, keep software updated, and remove old accounts from devices before donating, selling, or passing them to another child.

Posting, sharing, and the child's future autonomy

Adults often share about children for loving reasons: celebrating milestones,

asking for support, educating others, or staying connected with family. Still, "sharenting" can create a searchable history that the child did not choose. Before posting, consider whether the content reveals health information, toileting, tantrums, school difficulties, mental health concerns, disability details, location, or family conflict. Information that feels harmless now may feel intrusive to the child later.

A practical test is to ask: Would I be comfortable if this image or story appeared in a school presentation, a future job search, or a peer group chat? If not, keep it private. Consider sharing updates in smaller, trusted groups, removing metadata and location tags, using initials rather than full names, and asking older children for permission before posting identifiable content. Consent should be meaningful; a child should be allowed to say no without guilt.

For children with medical conditions, developmental differences, or mental health needs, privacy deserves extra care. Online communities can reduce isolation and help families find resources, but details such as diagnoses, medication histories, therapy reports, genetic information, or behavioral crises are sensitive. Discussing general experiences may be safer than posting identifiable clinical details. When in doubt, ask the child's healthcare professional about confidentiality, safeguarding, and documentation concerns.

Privacy, mental health, and safety concerns

Privacy problems can escalate into safety problems. Warning signs include a child becoming fearful of notifications, hiding screens in a distressed way, receiving messages from unknown adults, being pressured to keep secrets, losing sleep due to online conflict, or showing sudden mood changes linked to digital activity. These signs do not prove a specific diagnosis or event, but they do justify calm inquiry and support.

If a child reports cyberbullying, threats, unwanted sexual messages, extortion, or non-consensual sharing of images, respond with reassurance first. Avoid blaming language such as "Why did you send that?" or "I told you not to use that app." Save evidence when safe to do so, block or report the account, review platform reporting tools, and involve the school, pediatrician, mental health professional, or local safeguarding authorities when appropriate. If there is immediate danger, contact emergency services.

Privacy protection is not only technical; it is relational. Children are more likely to disclose problems when adults have been approachable during smaller mistakes. Regular, brief check-ins can help: "Anything online feel weird lately?" "Has anyone asked you to move to a private chat?" "Do you want help changing settings?" These conversations support both safety and emotional regulation without turning every device interaction into surveillance.

Working with schools, apps, and healthcare teams

Schools and healthcare-related services may use digital tools that collect sensitive information. Parents and caregivers can ask what data is collected, why it is needed, who can access it, how long it is retained, whether it is shared with vendors, and what happens if the family declines optional tools. For school platforms, ask about student privacy policies, breach notification procedures, and whether advertising or behavioral profiling is prohibited.

Healthcare portals, telehealth services, and therapy apps raise additional confidentiality questions, especially for adolescents who may have legal rights to private care in some settings. Families should ask clinicians how portal access works, what information parents can see, and how sensitive notes or messages are handled. Do not assume all health apps are regulated like clinical services; some wellness apps may collect extensive data without the same confidentiality standards.

A collaborative approach works best. Children need protection, but they also need practice making decisions. Create a family media agreement that covers privacy settings, downloads, passwords, photos, group chats, gaming, and what to do when something feels unsafe. Revisit it as the child matures. The aim is not perfect control; it is a layered system of trust, literacy, technical safeguards, and timely adult support.