

What to do when a child shares something online without permission



Start with calm containment

Discovering that a child has shared something online without permission can trigger an acute stress response in adults: rapid worry, anger, and a strong urge to seize the device or punish immediately. Try to pause before reacting. A child who feels humiliated may delete evidence, deny details, or avoid telling you about future online risks. The first goal is containment: keep the child emotionally available, establish what happened, and reduce further sharing.

Use a steady, specific opening such as: I need to understand what was posted and help fix it. We can talk about consequences after we know everyone is safe. This separates accountability from panic. For younger children, impulsive sharing may reflect immature executive function, meaning the brain systems for inhibition, future thinking, and risk appraisal are still developing. For adolescents, the issue may involve peer pressure, social reward, romantic dynamics, or misjudged privacy settings. None of this excuses harm, but it helps you respond in a way that teaches rather than only punishes.

Assess what was shared and who is affected

Next, identify the exact content, where it was shared, and who can access it.

Was it a family photo, another child's image, a screenshot of a private chat, a home address, a school name, a medical detail, a location tag, or financial information? The risk level changes depending on whether the post identifies a child, exposes sensitive personal information, or could invite harassment, grooming, identity misuse, or social humiliation.

Ask the child to show you the original post, direct message, group chat, or app activity without making them feel interrogated. Write down the platform, username, date, time, recipients, and whether the post was public, private, temporary, or reshared. If another child or adult is affected, consider their right to know, but avoid broadcasting the incident more widely than necessary. Protecting child online privacy includes data minimization: share details only with people who need them to remove content, safeguard a child, or provide support.

Limit the spread quickly

Speed matters because screenshots, downloads, and reposts can occur before a child understands the consequences. However, do not destroy all evidence if there is harassment, coercion, exploitation, or threats. In those situations, documentation may be important for school safeguarding staff, platform safety teams, or law enforcement.

Ask the child to stop posting, replying, or forwarding the content while you review the situation.

Take screenshots that show the content, account names, dates, times, URLs or platform identifiers if visible, and any threatening messages.

Delete or archive the child's post if it is safe to do so and evidence has been preserved when needed.

Use platform reporting tools for privacy violations, impersonation, harassment, sexual content involving minors, or non-consensual sharing of images.

Contact recipients calmly and ask them not to save, forward, or repost the material.

Review privacy settings for child accounts immediately afterward. Turn off public visibility, restrict comments and direct messages, disable location tagging, and check whether the account links to a school, sports team, address, or routine location. Location sharing in children can be especially sensitive

because it may reveal predictable movements.

Address consent, rights, and responsibility

Children often understand possession better than consent: they may think that because a photo is on their device, it is theirs to post. Explain that images, messages, health information, and embarrassing stories can affect another person's dignity, safety, and children's digital footprint long after the moment has passed. Consent should be specific, voluntary, and reversible where possible. Someone agreeing to a photo does not automatically mean agreeing to public posting, tagging, editing, or resharing.

In the United States, children's personal information online is partly addressed by the COPPA Rule, which requires certain online services directed to children under 13, or services that knowingly collect information from children under 13, to give parents notice and obtain verifiable parental consent before collecting, using, or disclosing that information. Families can use privacy notices and account settings to understand what data is collected and how it may be used. Outside the United States, privacy rules vary, but the ethical principle remains similar: children deserve involvement in decisions about their online presence as their maturity grows.

If the shared content involved another parent, a separated household, a school, or another child's family, keep communication factual and brief. The goal is repair and removal, not a blame spiral.

Teach repair without shaming

After the immediate risk is controlled, help the child make a repair plan. Repair may include apologizing, deleting content, asking others to delete copies, reporting reshared posts, and agreeing on future rules. The child should participate in age-appropriate ways because accountability is more effective when it is active rather than imposed. For example, a younger child might help draft a simple apology with a caregiver. An adolescent might contact a friend directly, but only if doing so will not worsen bullying or coercion.

Use the incident to teach developmentally appropriate internet safety. Ask practical questions: Who is in this image? Did every person agree to this exact

post? Could it reveal where someone lives, studies, worships, receives care, or spends time? Would it feel safe if a teacher, future employer, relative, or stranger saw it? These questions build metacognition, the ability to think about one's own thinking, which is still maturing through adolescence.

Model the same standard yourself. Before posting about your child, ask when possible, avoid embarrassing details, and respect a no. Adult behavior strongly shapes a child's expectation of privacy and consent.

Support wellbeing and know when to escalate

Some incidents are minor and become teachable moments. Others are safeguarding concerns. Escalate promptly if the shared material includes sexual images of a minor, threats, blackmail, stalking, grooming, hate-based abuse, self-harm content, or disclosure of a child's address or live location. If anyone is in immediate danger, contact emergency services. If the incident occurred through school peers, involve the school's safeguarding or wellbeing lead rather than expecting children to resolve it alone.

Watch the child's emotional response over the next days. Sleep disturbance, panic symptoms, school refusal, appetite change, withdrawal, tearfulness, irritability, or persistent shame may indicate significant distress, though these signs are not a diagnosis. A pediatrician, adolescent medicine clinician, psychologist, or licensed mental health professional can help assess risk, provide child disclosure support, and guide care if bullying, trauma, anxiety, depression, or self-harm concerns are present.

End with a prevention agreement that is concrete rather than vague: ask before posting others, no sharing screenshots of private chats, no location tags without permission, private accounts by default, and a trusted-adult network for mistakes. Online safety for children works best when children know they can ask for help early without losing all trust or connection.