



Digital Safety: Parental Attitudes and Controls

Technology, digital media, and online activities have become an integral part of day-to-day life across the globe. Usage of smartphones, laptops, tablets, and other information and communication devices (Internet connected technologies, or ICTs) is nearly universal, and access to these devices is becoming normalized among younger audiences. While this widespread access has provided advancements in communication, education, and entertainment, **it has also facilitated opportunities for exposure to sexually explicit material for children and teens.**

THIS RESEARCH BRIEF:

- Outlines the trends of increased technology use globally among youth.
- Describes some potential harms that children may encounter as they use technology.
- Reviews different actions parents are taking to mitigate the risks of their children experiencing or participating in harms facilitated by technology.
- Recommends strategies parents can use to increase their child's capability to operate online in safe and healthy ways.

TECHNOLOGICAL TRENDS AMONG TODAY'S YOUTH

It is estimated that one in three children globally is already an internet user. And when looking at the broader population, at any given time, a third of all internet users are children (under 18 years of age).¹ Internationally, mobile devices are how children are most commonly accessing the internet. Smartphone ownership and use has become a central part of teen life across genders, ethnicities, and socioeconomic backgrounds. According to the Pew Research Center, **95% of teens report owning a smartphone or have access to one.** Additionally, 45% of teens report they are online on a near-constant basis.² And while frequent ICT use is prevalent across various teen populations, daily screen time can vary among demographics. For instance, recent estimates of young people's screen time in lower-income homes reported an average of nearly two additional hours of screen media per day than peers in higher-income homes.³

The impact technology use and electronic media consumption have on the well-being of children has been investigated by many researchers and generated mixed reports.^{4,5} For instance, research has revealed how **healthy internet habits can correlate with positive outcomes such as academic achievement, literacy, and even cognitive development.**⁶ Digital media and technology can also supply youth with information and education regarding sexual health and development that may have otherwise been unavailable, particularly among low-income populations. Increased usage of technology also coincides with inherent risk of harmful encounters with material that is neither age-appropriate nor accurate.

POTENTIAL HARMS FACILITATED THROUGH TECHNOLOGY

Increased online activity and technology use among children and youth can **facilitate exposure to content that may adversely impact a youth's sexual education, behaviors, and attitudes.**⁷ Additionally, parents and caregivers should be aware individuals online may target vulnerable children and teens via the technology that is ever-present in their daily lives. And while some of these harms are perpetrated by older teens or adults, they can also be perpetrated by a youth's peers. Such peer victimization has been attributed, in part, to **increased levels of problematic internet use** among children and adolescents, which may be exacerbated by the online disinhibition effect.^{8,9}

Given these valid concerns, it is no surprise then that most parents express discomfort or distress regarding their children's engagement with digital media and technology. One study showed that 65% of parents experience concern over the types of experiences their child or teen is encountering via ICTs. The same study showed that nearly six out of ten parents routinely check their child's browsing history and/or text messages.¹⁰ Researchers suggest that **such concerns among parents are indeed merited**, especially as ICTs continue to become more intrinsic to daily connections and functioning.⁹

Parents and caregivers commonly express feeling inadequately equipped to address the following elements of their child's online experience:¹¹

- Managing the pressures and impacts of increased social media activity.
- Early exposure to mature content.
- Excessive screen use.
- Struggling with or an inability to have in-person interactions.
- Cyberbullying.
- The exchanging of explicit messages and images.

SEXUALLY EXPLICIT CONTENT

Sexually explicit content, which includes what many term as “pornography,” has been made available to younger audiences through the widespread use of ICTs.

This access increases the risk of children's early exposure to graphic sexual material, whether intentionally or through accidental encounters. Such exposure remains prevalent among youth across demographics, backgrounds, and geographic locations. One 2016 study in the UK found that **among the 11- to 16-year-olds they surveyed, 53% had viewed sexually explicit material at least once.** Of this sample, 94% had been exposed to such material before the age of 14.¹²

Early exposure to explicit material is not only age-inappropriate but can also lead to adverse effects in a youth's sexual development. Sexually explicit content found online often **portrays inaccurate and violent depictions of sexual behaviors**, and the consumption of such materials can adversely impact the sexual attitudes, behaviors, and expectations among children and teens.^{7, 13} This is especially the case if engaging with explicit themes becomes a sustained pattern at a young age. Repeated viewing of sexually explicit materials may distort a young person's view of sexual relationships, gender roles, and increase the likelihood of youths demonstrating sexist attitudes and perpetuating harmful stereotypes within their own relationships.^{14, 15}

PARENTAL ATTITUDES AND CONTROLS

While most parents feel that the benefits of their child being online outweigh the potential harms, they generally report chief concern over protecting children from inappropriate material or persons with malintent.¹⁶

Parental controls to mediate their children's interactions with potential harms can take various forms: restricting technology use or access to devices; limiting screen time;¹⁷ outlining approved activities; establishing home rules and expectations revolving around technology use;¹⁸ restricting use through technical means (content filters, network access limits, etc.);⁷ monitoring use through technical means (surveillance, checking online activities, logs of accessed media, etc.); and engaging with children to educate them about the risks/benefits of various online activities.¹⁹

While no single strategy will eliminate risk, **it is important for parents to consider the individual circumstances of their child and what controls may help to mitigate risky behavior**—particularly with children who lack maturity or struggle with problematic internet use.²⁰

Parenting styles and confidence can vary according to education, socio-economic status, cultural background, and geographical location.²¹ Parents with the highest confidence in managing their child's technology use are also most likely to believe that they know more than their child does about technology and online activities. Investigation on parent awareness of online risks reaffirmed **the importance of the parent-child relationship in dealing with a child's negative online experiences**. Sampled parents reported that a child's disclosure of a harmful encounter was the primary way they found out about these experiences. The next most common way parents found out about their child's online experience was through their own investigation or through reports from their spouse or partner.

It should be noted that children often report encountering objectionable content and negative online experiences outside the home. Evidence suggests that household-level filtering is generally ineffective in reducing the chance of children from ever encountering adverse online experiences, partly because of the ubiquitous nature of internet availability away from home.^{22, 23} Furthermore, parents should consider the merits of the argument that “by limiting their access to [a broader] range of content, users are not learning the information literacy skills that afford genuine and sustainable protection in the digital arena.”²⁴ **While filters and controls can be a helpful tool, they should not be viewed as fool-proof or a permanent solution to entirely mitigate online risks.**

CONCLUSION AND RECOMMENDATIONS

ICTs have become an integral component of 21st-century living; the impacts of this integration will continue to shape the social developments, trends, behaviors, and relationships among youth. While proactive parents understand that there are certain activities that carry unduly high risk and should wisely be avoided, they acknowledge the reality that children and youth expect (and in many cases are required) to operate in a digital environment and abstaining from all online activities is not a reasonable solution. **Thus, parents and mentors should actively help to prepare children for a wide spectrum of encounters (positive and negative)**. We recommend preparing children by orienting them to the risks that are present for the online activities they will be participating in, along with strategies for navigating away from offensive material and getting support to identify potentially harmful situations.

Educating and orienting children to the online landscape is a critical foundation for any strategy.¹⁵ In this vein, **parents can teach and model what a healthy relationship with technology looks like**, not only in terms of what content they consume, but also what content they create and what identity they present to others.⁸ A media use plan will help a child better understand the importance of digital citizenship and the magnitude of their digital footprint. As parents provide a supportive role along with the expressed goal of helping children self-regulate their internet and social media use, young people can develop the “online resilience” and “digital optimism” needed to take advantage of the positive aspects of the internet and steer clear of potential harms.

Monitoring and supervision strategies can be tailored to the specific circumstances for children who are accessing social media and other online content. For some children, simply identifying the risks and showing them how to navigate around or away from harmful material/situations will be sufficient. For those who are more prone to engage in risky behaviors, a more direct approach might be needed to alert parents and caregivers when boundaries are crossed (see “Controls” section above).

While parental enforcement of controls regarding technology is crucial, it may also spur potential tension with the child. For this reason, **controls should be applied judiciously**, as fractures in the child-parent relationship can prompt additional complications or even more online risky behavior. **We do not endorse parents threatening a complete withdrawal of “internet privileges” as a negative consequence** (research demonstrates that such threats act as a barrier to future communications where a child needs help), but parents could consider the option to closely monitor online activity until the child builds trust and confidence in their ability to engage online in a healthy way.

Pairing this education with well-understood boundaries and value-based expectations is a natural extension for any behavior (online or otherwise). Discussions about boundaries, consent, empathy, privacy, communication, and healthy sexual behaviors will not only help increase a child's digital literacy but will also increase their resilience and autonomy in other areas of life. As many ICT-facilitated harms occur in conjunction with offline harms,²⁵ and can yield similar adverse impacts, **the support and two-way communication a parent fosters in the home are essential** to the child's ability to navigate through difficult situations, both online and offline.⁸

Ultimately, parents who want to proactively protect their children can take the following researched-based actions: enabling their children's capacity through critical thinking, empathy, and high self-esteem; fostering the technical capabilities of their children (and others they interact with) to establish well-informed security measures and monitoring strategies; promoting constructive two-way communication between peers and adults; and accentuating positive peer status, academic performance and mentorship, which can act as barriers to online abuse.¹⁹

APPENDIX A—RECOMMENDED INTERVENTIONS

PRIMARY MESSAGING TO PARENTS

1. Teach and model digital literacy.

- a. Help your child learn to navigate and regulate equitable, age-appropriate ICT use.
- b. Learn about risky internet behaviors and their potential harms. Teach your child about them and their adverse effects—for all parties involved.
- c. Educate children on recognizing sexually inappropriate advances or solicitations—whether in-person or online—and how to navigate around such encounters.
- d. Initiate frequent, open discussions about sexually explicit content and what your child can do when they encounter such content.

2. Enforce structure around ICT-use.

- a. Clearly and consistently communicate boundaries around screen times, access to devices, what constitutes appropriate content, online activities, social media engagements, and other conditions of technology use.
- b. Monitor internet use, including the ICTs your child uses, the accounts and profiles they've created, and the sites and social media channels they frequent.
- c. Determine what security measures, filters, and other controls/supervision you want to implement on your child's ICTs. As your child matures, involve them in identifying and employing safe strategies.
- d. Be aware of which adults can communicate to your child via ICTs and monitor their communications.
- e. With any approach, be mindful of guiding youth toward the eventual goal of being capable independent digital users.
- f. Avoid penalizing children with the complete withdrawal of their digital privileges.

3. Build communication and trust.

- a. Educate and model the importance of boundaries, consent, regulation, communication, and other skills essential to your child's autonomy in online and offline spaces.
- b. Within the boundaries you have set, allow your child the space and opportunity to familiarize themselves with ICTs in order to help build their skills in digital literacy and participate in meaningful engagements online.
- c. Inquire after your child's questions, concerns, and curiosities related to tech-facilitated interactions, content, and behaviors. Listen with empathy and openness to their disclosure of any missteps.

PRIMARY MESSAGING TO COMMUNITIES

1. Model parental interventions.

- a. Educate parents and caregivers about the importance of having frequent, open conversations with their children about the sexually explicit content they will inevitably encounter via ICTs, and how the child may feel and/or respond when they come across such content.
- b. Prompt other parents and caregivers to examine their own relationship with ICTs, their views regarding sexual content, and what factors (cultural values, religious beliefs, etc.) contribute to those views.
- c. Explain what a media use plan is, why it is helpful in increasing digital safety, and how it can be effectively implemented in the home.

2. Raise awareness around internet controls.

- a. Clarify that while internet filters and other security measures can be useful tools in mitigating tech-facilitated risks, they should not serve as substitutes to more effective protective factors, like open communication, modeling healthy regulation, and fostering a safe and supportive home environment.
- b. Help connect parents with tools that identify/bring awareness to websites, platforms, and apps that are likely to place a child's safety at risk.
- c. Collaborate with educators and other community members to help address, examine, and/or improve the security measures being implemented at schools and other youth-serving organizations in your area.

PRIMARY MESSAGING TO MEDIA

1. Help parents make more insightful decisions around the content they consume and encourage.

- a. Provide ratings, warnings, and descriptions that accurately convey the maturity level and targeted audience of the content being presented.
- b. Use transparency to clearly communicate the criteria assigned to blanket terms such as "kid friendly," "general audiences," and "TV-MA."
- c. Ensure audience settings for streaming services and multimedia platforms are accessible, transparent, and easy to adjust.

2. Educate and raise awareness around solution-based efforts.

- a. When promoting security measures such as filtering systems, clarify that children are still at risk of encountering harmful content and/or behaviors even with such measures in place.
- b. Call out trends, sites, platforms, and apps that may increase the risk of a child experiencing technology-facilitated harm and what parents can do to combat such risks.
- c. Raise awareness around legislation policies, community events, parental education initiatives, and other solution-based efforts around reducing the risk of technology-facilitated harms

APPENDIX B—KEY STATISTICS AND ADDITIONAL RESOURCES

KEY STATISTICS

- 53% of 11–16-year-olds report seeing online pornography at least once. Of this sample, 94% report viewing online pornography before age 14.¹²
- 95% of teens report owning a smartphone or having access to one.²
- In 2020, about 4.67 billion people (59% of global population) were active internet users.²⁶
- 45% of teens report that they are online almost constantly.²⁷
- Adolescents who report having a positive relationship and open communication with their parents engage in fewer risky sexual behaviors, online and offline.⁸

ADDITIONAL RESOURCES

- Thorn.org <https://parents.thorn.org/situation/>
- AMAZE.org <https://amaze.org/?topic=personal-safety>
- Global Kids Online <http://globalkidsonline.net/updates/>
- Social Media Safety <https://www.rainn.org/safe-media>
- Teaching Digital Citizens in Today's World https://d1e2bohyu2u2w9.cloudfront.net/education/sites/default/files/tlr_component/common_sense_education_digital_citizenship_research_backgroundunder.pdf
- Everything You Need to Teach About Digital Citizenship <https://www.common sense.org/education/digital-citizenship>

APPENDIX C—GLOSSARY OF TERMS

Digital footprint is the record of data generated through online activities linked back to a specific person. This can include a user's browsing/search history, images/messages they post or send (even deleted ones), content they "liked" on social media, and online profiles they create.

Digital literacy describes a person's level of technical and social ability specifically used to navigate the online environment in an effective way. Understanding and practicing safety during online activities is a key component of digital literacy.

Filters are controls or measures that restrict an internet user from accessing certain websites or content. "Underblocking" occurs when a filter incorrectly allows a user to access text or images that should be blocked. "Overblocking" occurs when a filter doesn't allow content to be shown that is, in fact, suitable for the user.

Internet of Things (IoT, loT): includes smart-devices (cameras, TVs, speakers, appliances, etc.) that are connected to the internet and are often found in the home.

Media use plans are one way that parents can work with their children to establish defined expectations relating to how they consume media or use technology. Effective media use plans outline appropriate online *content*, *conduct*, and what to do when a child encounters a challenge.

Online disinhibition effect: when people say and do things online that they wouldn't ordinarily say and do in the face-to-face world.

Problematic internet use (noted as PIU in academic literature) occurs when an individual's preoccupation with online activities results in social, occupational, or financial difficulties. In some cases, pathological behavior connected with internet use is present.

Screen time is a common expression that measures the amount of time spent using any computer, television, mobile device, or game console.

APPENDIX D—RISKY ONLINE BEHAVIORS

RISKY ONLINE BEHAVIORS

- Visiting sites with content intended for adults (e.g., pornography).
- Sending/receiving sexually explicit images.
- Having sexual conversations with adults.
- Posting personal information about yourself or others.
- Providing financial information to unsecure sites.
- Visiting sites with smart feeds or recommendations that continue to provide content automatically (e.g., Youtube's video algorithm and continuously streamed video services).
- Accepting friend requests from strangers on social media.
- Sharing your address or current location with others online.
- Having public profiles that can be viewed by anyone.
- Creating social media accounts that parents are not aware of.
- Using gaming applications or services that allow chats or unmonitored communication.
- Access to accounts where unmonitored purchases can be made.

REFERENCES BY AUTHOR

- Anderson, E. L., Steen, E., & Stavropoulos, V. (2017). Internet use and problematic internet use: A systematic review of longitudinal research trends in adolescence and emergent adulthood. *International Journal of adolescence and youth*, 22(4), 430-454.
- Cooke, L., Spacey, R., Muir, A., & Creaser, C. (2014). Filtering access to the internet in public libraries: An ethical dilemma? In Presig, A.V., Rosch, H., & Stuckelberger, C. (Eds.). *Ethical dilemmas in the information society: How codes of ethics help to find ethical solutions*. Geneva: globalethics.net (pp. 181-192).
- Coyne, S. M., Ward, L. M., Kroff, S. L., Davis, E. J., Holmgren, H. G., Jensen, A. C., ... & Essig, L. W. (2019). Contributions of mainstream sexual media exposure to sexual attitudes, perceived peer norms, and sexual behavior: A meta-analysis. *Journal of Adolescent Health*, 64(4), 430-436.
- Daoud, R., Starkey, L., Eppel, E., Vo, T. D., & Sylvester, A. (2020). The educational value of internet use in the home for school children: A systematic review of literature. *Journal of Research on Technology in Education*, 1-22.
- Duckert, M., & Barkhuus, L. (2021, June). To Use or Not to Use: Mediation and Limitation of Digital Screen Technologies within Nuclear Families. In *ACM International Conference on Interactive Media Experiences* (pp. 73-83).
- Family Online Safety Institute (FOSI). (2014). Parenting in the Digital Age: How Parents Weigh the Potential Benefits and Harms of Their Children's Technology Use
- Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2020). Youth internet safety education: aligning programs with the evidence base. *Trauma, Violence, & Abuse*, 1524838020916257.
- Hinkley, T., Verbestel, V., Ahrens, W., Lissner, L., Molnár, D., Moreno, L. A., ... & Idefics Consortium. (2014). Early childhood electronic media use as a predictor of poorer well-being: a prospective cohort study. *JAMA pediatrics*, 168(5), 485-492.
- James, C., Weinstein, E., & Mendoza, K. (2021). Teaching digital citizens in today's world: Research and insights behind the Common Sense K–12 Digital Citizenship Curriculum. (Version 2). San Francisco, CA: Common Sense Media.
- Johnson, Joseph. (2021). Worldwide digital population as of January 2021. Statista.
- Livingstone, S., Winther, D. K., & Saeed, M. (2019). *Global kids online comparative report* (No. inorer1059).
- Martellozzo, E., Monaghan, A., Adler, J. R., Davidson, J., Leyva, R., & Horvath, M. A. (2016). "I wasn't sure it was normal to watch it..." A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people.
- May-Chahal, C. A., & Palmer, C. E. (2018). Rapid evidence assessment: Characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation.
- Mitra, Dakhina. (2020). Keeping Children Safe Online: A Literature Review. *Centre for Excellence in Child and Family Welfare*.
- Morris, M. E. (2020). Enhancing relationships through technology: directions in parenting, caregiving, romantic partnerships, and clinical practice. *Dialogues in Clinical Neuroscience*, 22(2), 151.
- Office of eSafety Commissioner (Australia). (2019). Parenting in the Digital Age.
- Orben, A., & Przybylski, A. K. (2019). The association between adolescent well-being and digital technology use. *Nature Human Behaviour*, 3(2), 173-182.
- Pew Research Center. (2018). "A Majority of Teens Have Experienced Some Form of Cyberbullying." [1]
- Pew Research Center. (2019). "How Parents Feel About—And Manage—Their Teens' Online Behavior and Screen Time."
- Pew Research Center. (2020). "Parental Attitudes—And Experiences—Related to Digital Technology."
- Pew Research Center. (2018). "Teens, Social Media & Technology 2018." [2]
- Pontes, H. M., Kuss, D. J., & Griffiths, M. D. (2015). Clinical psychology of Internet addiction: a review of its conceptualization, prevalence, neuronal processes, and implications for treatment. *Neuroscience and Neuroeconomics*, 4, 11-23.
- Przybylski, A. K., & Nash, V. (2017). Internet filtering technology and aversive online experiences in adolescents. *The Journal of pediatrics*, 184, 215-219.
- Przybylski, A. K., & Nash, V. (2018). Internet filtering and adolescent exposure to online sexual material. *Cyberpsychology, Behavior, and Social Networking*, 21(7), 405-410.
- Quadara, A., El-Murr, A. & Latham, J. (2017). *The effects of pornography on children and young people: An evidence scan*. (Research Report). Melbourne: Australian Institute of Family Studies.
- Wright, P. J., Tokunaga, R. S., & Kraus, A. (2016). A meta-analysis of pornography consumption and actual acts of sexual aggression in general population studies. *Journal of Communication*, 66(1), 183-205.
- Wurtele, S. K., & Kenny, M. C. (2016). Technology related sexual solicitation of adolescents: A review of prevention efforts. *Child Abuse Review*, 25(5), 332-344.

REFERENCES BY NUMBER

01. Livingstone, 2019
02. Pew Research Center, 2018 [1]
03. James, 2021
04. Hinkley, 2014
05. Orben, 2019
06. Daoud, 2020
07. Quadara (2017)
08. Wurtele, 2016
09. Pontes, 2015
10. Pew Research, 2019
11. Pew Research Center, 2020
12. Martellozzo, 2016
13. Coyne, 2019
14. Wright, 2016
15. May-Chahal, 2018
16. Family Online Safety Institute, 2014
17. Morris, 2020
18. Duckert, 2021
19. Mitra, 2020
20. Anderson, 2017
21. Office of eSafety Commissioner, 2019
22. Przybylski, 2017
23. Przybylski, 2018
24. Cooke, 2014
25. Finkelhor, 2020
26. Johnson, 2021
27. Pew Research Center, 2018 [2]