# Digital Safety for Children with Intellectual Disabilities When Using Mobile Devices from Parents' and Teachers' Perspectives

Anonymous Author(s)

## ABSTRACT

As mobile devices become increasingly integrated into children's daily lives, digital safety has emerged as a pressing concern, particularly for children with intellectual disabilities (ID), who are more vulnerable due to their cognitive and behavioral challenges. Despite their heightened risk, little research has addressed the unique digital safety issues these children face. To bridge this gap, we conducted semi-structured interviews with parents and special education teachers who are key figures for overseeing the digital access and safety of children with ID. Our findings highlight four primary concerns: imitation of harmful behaviors, accidental misoperation of devices, risks from frauds, and exposure to cyberbullying. To address these, parents and teachers largely rely on proactive educational strategies supported by technical controls and device restrictions. We conclude by emphasizing the need to adapt special education practices to the evolving digital landscape and propose inclusive safety strategies applicable to other at-risk user groups.

## CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

## KEYWORDS

Digital safety, Children with special needs, Children with intellectual disability, Vulnerable group, Security and Privacy

**ACM Reference Format:**

Anonymous Author(s). 2018. Digital Safety for Children with Intellectual Disabilities When Using Mobile Devices from Parents' and Teachers' Perspectives. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (Conference acronym 'XX)*. ACM, New York, NY, USA, 18 pages. https://doi.org/XXXXXXX.XXXXXXX

## 1 INTRODUCTION

In the digital age, mobile devices represented by smartphones, tablets, and smartwatches [72, 121] have been deeply integrated into children's daily lives, providing a wealth of resources for education, entertainment, and social interaction [92, 124]. While it brings benefits, this integration also introduces significant digital safety risks—ranging from harmful content and online predators to cyberbullying and financial scams [42]. Previous research has summarized the common types of risks children encounter in digital environments, including content threats (e.g., pornography, violence), contact threats (e.g., sexual extortion), and conduct threats (e.g., cyberbullying, harassment), known as the 3Cs [82]. Subsequent studies have expanded 3Cs to include a new category of risk—contract threats (e.g., financial fraud) [84]. Exposure to such risks can result in serious consequences for children, including emotional distress, anxiety, and in severe cases, self-harm or suicide [4].

To protect children online, researchers have focused heavily on the roles of parents and teachers, who act as the primary gatekeepers of digital safety [25, 85, 91]. Parental strategies, such as setting usage restrictions and discussing online behavior, are formalized in models like the Teen Online Safety Strategies (TOSS) framework, which categorizes involvement into monitoring, restrictive mediation, and active mediation [144]. Teachers also play a crucial role, often through classroom discussions about digital safety and the use of third-party monitoring tools [65, 91], such as tracking students' browsing history and monitoring the language used in email communications to detect any risky behavior [21, 122].

However, one vulnerable subgroup—children with ID—remains largely neglected in this body of research. For these children, safety threats in digital environments may be amplified due to their inherent vulnerabilities [29]. According to the World Health Organization (WHO) and the American Association of Intellectual and Developmental Disabilities (AAIDD), children with ID have significant impairments in intellectual functioning and adaptive behavior [147]. These impairments present significant challenges for children with ID in multiple activities, including difficulties in reasoning, judgment, problem solving, abstract thinking, learning from experience, communication, and social interaction [33]. These challenges not only constrain their daily life and learning activities but also exacerbate their susceptibility to digital threats [87].

Despite their heightened vulnerability, children with ID have received little attention in digital safety research, particularly in the context of their increasing use of mobile devices [6, 44]. While some studies have explored digital risks and protective strategies for other at-risk groups—such as the elderly [96, 101], people with visual impairments [89, 139], or racial minorities [18]—the unique challenges faced by children with ID remain underexplored. Most existing safety frameworks are designed for typically developing children [42], leaving a significant knowledge gap regarding how parents and teachers—who serve as the primary digital safety guardians for children with ID—understand and address these risks [86, 104, 111].

Therefore, we aim to explore how parents and teachers perceive and address the digital safety risks faced by children with ID. By examining their experiences, we aim to identify the specific safety challenges these children face when using mobile devices and to uncover the educational and technical strategies used to protect them. These perspectives from parents and teachers provide crucial insights for designing more inclusive and effective safety solutions



*Conference acronym 'XX, June 03–05, 2018, Woodstock, NY*



ACM ISBN 978-1-4503-XXXX-X/18/06
https://doi.org/XXXXXXX.XXXXXXX

tailored to this vulnerable group. This leads us to pose the following research questions (RQs):

**RQ1:** What safety concerns do parents and teachers perceive regarding mobile device usage by children with ID?

**RQ2:** How do parents and teachers guide and address the safety concerns of mobile device usage by children with ID?

To address these RQs, we conducted semi-structured interviews with parents ($n_1$ = 12) and special education teachers ($n_2$ = 10) in China. We explored their perspectives on how children with ID interact with mobile devices, the specific digital risks they encounter, and the strategies used to manage these risks.

From our analysis, four primary categories of digital safety concerns emerged: (1) Inappropriate imitation of harmful behaviors, (2) Misoperations causing financial loss, (3) Frauds such as scams or malicious contact, and (4) Cyberbullying rooted in the children's visible or behavioral differences. Among these, parents and teachers were particularly worried about children imitating violent behavior they saw online, which could lead to misunderstandings or exclusion by peers. In contrast, they expressed less concern about some of the more commonly studied risks in typically developing children, such as exposure to pornography, due to these children's reduced cognitive ability to interpret such content.

To mitigate these concerns, our findings indicate that parents and teachers tend to rely on a combination of educational strategies and technical management strategies. Educational strategies are centered around helping children build awareness and understanding through concrete, sensory-driven experiences, as opposed to verbal explanations or abstract warnings, which are often ineffective for this group. When educational efforts fall short, parents and teachers often turn to technical management strategies—restricting device functions, disabling certain features, or cutting off internet access entirely—to ensure the children are not exposed to harmful content or features they cannot navigate safely.

In comparing these findings to existing literature on typically developing children, we discussed the similarity and uniqueness of concerns expressed by parents and teachers regarding the digital safety of children with ID. Additionally, we further discussed the potential challenges of current safety strategies employed by parents and teachers in the digital environment, calling for a reassessment and adjustment of existing safety frameworks in the fields of special education and safety design. Furthermore, we proposed potential methods to improve existing designs and develop new digital safety education tools to better support children with ID in navigating digital environments more safely.

This study contributes two significant insights to the field of security usability research. First, it elucidates the digital safety risks parents and teachers perceive for children with ID. This understanding pinpoints the digital safety needs of children with ID, establishing an empirical foundation for developing more inclusive safety frameworks. Second, it identifies mitigation strategies driven by parents and teachers that incorporate both educational interventions and technical adaptations. These strategies offer new perspectives for designing safety solutions that respect educational theories, as well as for constructing a defensive system for the digital practices of a broader at-risk user group.

# 2 BACKGROUND

## 2.1 Mobile Devices Usage by Children

Mobile devices have become deeply integrated into, and now dominate, the daily lives of children [19, 37], shaping their access to learning, communication, and entertainment [102, 118]. Children use a variety of mobile devices, including tablets [55], smartphones [113], laptops [68], smartwatches [31], and gaming devices [107]. Their main activities on mobile devices include watching videos [63], playing games [72], using social media [37], and engaging in mobile learning through educational apps [112], which together shape their daily digital experiences.

## 2.2 Children with ID

According to WHO [33, 147] and AAIDD [127], ID is defined by significant limitations in both intellectual functioning and adaptive behavior. Intellectual functioning refers to general cognitive abilities such as reasoning, learning, and problem-solving, while adaptive behavior encompasses practical, social, and conceptual skills essential for daily living. These deficits manifest during the developmental period and significantly impair the child's capacity for independent functioning. Children with ID typically experience a constellation of interrelated developmental challenges that affect their cognitive processing, motor coordination, communication abilities, social interaction skills, and physical characteristics.

A key area of difficulty is cognitive processing, where children with ID may struggle with memory, abstract reasoning, and logical thinking. Their ability to interpret and respond to stimuli is often diminished, which may affect both learning and risk awareness in digital settings [59, 132].

In addition, many children with ID exhibit motor coordination issues, such as clumsiness or difficulty with fine motor tasks. These motor impairments can manifest as awkward movements or repetitive behaviors that serve no clear purpose, potentially impacting their ability to use digital interfaces effectively [50, 79].

Communication delays are another common feature. These include both speech difficulties—such as unclear pronunciation—and broader language challenges, including understanding grammatical structures, grasping the meanings of words, or trouble forming sentences [90, 100]. As a result, these children potentially face difficulties in understanding online content.

Additionally, deficiencies in social interaction skills lead to social communication challenges for children with ID. Children with ID may struggle to engage in conversations, recognize social cues, or adjust their behavior appropriately in different social contexts, which may increase their vulnerability to online contact [117, 129].

Furthermore, many children with ID also experience physical health conditions, such as facial or limb abnormalities, sensory impairments (e.g., visual or auditory), and other chronic medical issues. These traits not only affect development but may also impact their social well-being [70, 136].

Due to the range and severity of these challenges, children with ID often require structured educational support tailored to their individual needs [70]. Three main types of educational settings are typically used. Some children attend special education schools, where the curriculum is designed to build life skills and promote

independence through foundational cognitive training [70]. Others receive instruction in rehabilitation centers, which combine sensory integration therapy with functional academics to enhance learning and adaptability [119]. For children with milder forms of ID, inclusive education in mainstream schools is sometimes an option. This model offers opportunities for greater peer interaction while still providing targeted support services [20].

# 3 RELATED WORK

## 3.1 Digital Safety Risks for At-Risk Users

Recent research has increasingly emphasized the need to understand how digital environments uniquely impact at-risk populations—groups whose individual characteristics or life circumstances increase their vulnerability to harm online. These users often face higher exposure to digital threats and experience disproportionately severe consequences compared to the general population [10, 138]. This growing body of work serves as an important foundation for exploring the specific vulnerabilities of children with ID.

Various at-risk groups have been the focus of prior research, including LGBTQ+ individuals, survivors of intimate partner violence, elderly users, and people with disabilities. Each group faces a distinct set of digital safety risks. For instance, LGBTQ+ individuals frequently experience targeted harassment, online hate speech, and identity-based attacks [2, 14, 47]. Survivors of domestic abuse are often monitored through spyware and location-tracking apps, enabling abusers to continue exerting control even after physical separation [43, 51, 93]. Older adults with cognitive decline may have difficulty distinguishing between malicious behavior and simple user error, making them prime targets for phishing and scams [96, 101]. Visually impaired users may inadvertently expose private information in public spaces due to the loud and visible nature of assistive technologies like screen readers [89, 139].

Across these groups, some digital safety challenges are shared. Many at-risk users struggle with recognizing online risks, making safe decisions, or using protective technologies effectively [39]. Cognitive load [101], low digital literacy [54], and reliance on others for online navigation [77] are common barriers across children, the elderly, and individuals with disabilities [105, 106]. These users also tend to lack direct control over the technologies they use, placing greater weight on the role of caregivers, institutions, or platform designers in shaping their online safety [77].

However, each group also faces unique vulnerabilities. For children with ID, digital risks are shaped by core developmental characteristics—such as impulsivity, limited abstract reasoning, and underdeveloped language and social skills [75, 84, 143, 149]. These traits may lead to risky behaviors, such as engaging in unsafe actions without understanding the potential consequences [29, 40, 60, 104], which is distinct from the typical developmental behavior of children who may intentionally test boundaries online [66, 145].

Despite these vulnerabilities, children with ID remain significantly underrepresented in digital safety research. While prior studies have examined how these children use technology—for learning, communication, or entertainment [30, 126]—they rarely explore the specific threats they encounter online or the strategies parents and teachers use to protect them. This absence of focus is especially concerning given that parents and teachers play a crucial role as the primary digital gatekeepers for these children [25, 76, 88, 91]. To address these gaps, we pose the following RQ:

**RQ1:** What safety concerns do parents and teachers perceive regarding mobile device usage by children with ID?

## 3.2 Strategies to Protect Children's Digital Safety

Protecting children in digital environments has been a central concern across fields such as computer science, cybersecurity, and education. Researchers and practitioners have proposed a range of strategies to mitigate risks, which broadly fall into two categories: technical strategies and nontechnical, caregiver-led strategies.

Technical approaches are designed to detect, restrict, or block harmful content and interactions. These include AI-driven content filters [34, 115], age-verification systems [125], real-time behavioral monitoring tools [148], and communication protocols that ensure safer messaging environments [69]. Automated detection systems have also been developed to identify abusive content or suspicious behavior on social platforms [5]. In addition, interface designs tailored to children—such as simplified layouts or usage constraints—have been proposed to help reduce exposure to inappropriate content and ease cognitive load [120].

Alongside these technical tools, non-technical strategies—often led by parents and teachers—play an essential role in safeguarding children's online activities. Children frequently rely on adult supervision and guidance to navigate digital spaces, especially during early developmental stages or when encountering unfamiliar content [25, 42, 91, 138]. Parents and teachers typically implement practical safety measures such as monitoring screen time [91], restricting access to specific apps [42], reviewing browsing history, and setting ground rules for online behavior [7]. Many also engage in proactive education, using open conversations, classroom discussions, and structured lessons to raise children's awareness of digital risks and responsible usage [36, 65].

Despite the central role parents and teachers play in protecting children online, most existing research focuses on strategies used with typically developing children. These studies often assume that children possess a certain level of comprehension, communication ability, and digital awareness—assumptions that may not apply to children with ID [27, 90, 90]. For these children, general safety guidance may be difficult to understand, and protective systems may not be cognitively accessible without modification.

While the broader literature acknowledges the importance of parents' and teachers' mediation, there remains a critical gap in understanding how they support children with ID in managing digital risks. We know little about the strategies they implement or how they adapt conventional tools and educational techniques to meet the needs of children with ID. This leads to our second RQ:

**RQ2:** How do parents and teachers guide and address the safety concerns of mobile device usage by children with ID?

# 4 METHODOLOGY

## 4.1 Positionality Statement

As qualitative research positions the researcher as the primary data collection instrument [17], our work is inherently shaped by the

authors' identities and experiences [8, 13]. None of the authors are individuals with ID, and our understanding derives exclusively from the perspective of parents and teachers. We acknowledge that this indirect lens cannot represent the first-hand lived experiences of children with ID. However, our interdisciplinary expertise in special education, child developmental psychology, and information technology security enables contextualization of developmental profiles, identification of technology-mediated risks, and design of methodologically sound approaches. Through rigorously designed interviews and thematic analysis, we prioritize authentic representation of caregiver insights. Ultimately, we commit to translating these findings into actionable strategies that safeguard digital well-being and advance equitable digital inclusion for children with ID.

## 4.2 Ethical Considerations

This study was conducted in China under approval by the Institutional Review Board (IRB) at [***] (redacted for review). Its design adheres to the ethical principles outlined in the Belmont Report [1]: respect for persons, beneficence, and justice.

The principle of respect for persons was integrated into the informed consent process: before the interview, participants received a consent form. This form detailed the interview procedures, audio recording requirements, data handling procedures and usage, and their rights. These rights included the option to decline answering questions, withdraw at any time, and receiving compensation for the interview. By providing this information upfront and ensuring autonomy, the research respects participants' self-determination and right to make informed decisions about their involvement.

In line with beneficence, our study was designed to reduce harm while maximizing benefits for both participants and the broader caregiver community. Recognizing that caregivers of children with intellectual disabilities may be vulnerable to psychological distress—stemming from stigmatization or emotional discomfort when discussing their child's condition [24, 103]—we implemented targeted safeguards. Questions about the child's condition were limited to essential demographic data and phrased neutrally (e.g., "your child") to avoid stigmatizing language. Participants were also reminded of their right to skip questions or withdraw at any time, ensuring their control. Although direct benefits to individuals may be limited, the study aims to deepen understanding of caregiver challenges and inform the development of improved support systems, resources, or policies, thereby aligning with the principle of beneficence by minimizing harm and pursuing long-term benefits.

The principle of justice guided our research through fair, inclusive participant selection and a commitment to ensuring that benefits reach those involved. We recruited caregivers of children with ID using an unbiased process—irrespective of socioeconomic status, race, or other factors—so that no subgroup bears disproportionate burdens. Moreover, justice demands that those who participate also benefit from the research. Though immediate policy changes are not guaranteed, our study aims to generate insights that highlight caregivers' needs and support improved resources or practices, aligning benefits with participants' interests.

## 4.3 Recruitment and Demographics

We employed a mixed-methods recruitment approach, combining direct recruitment and snowball sampling. We posted recruitment information on various online social platforms, including WeChat public accounts, WeChat groups, and Xiaohongshu, which have hundreds of millions of active users[1].

Initially, we received responses from 15 potential participants (10 parents and 5 teachers). Each of them was screened to ensure they met our inclusion criteria. For parents, the criteria required that their child is medically diagnosed with an ID, is under 18, and has experience using mobile devices. For teachers, candidates must currently or have previously worked at a special education school or an institution for ID rehabilitation, hold a core teaching role, and have direct experience interacting with or managing children with ID. Detailed information provided in Appendix A. Three parents were excluded because their children had not used any mobile devices. Ultimately, the direct recruitment strategy identified 12 participants (7 parents and 5 teachers).

During the interviews, we asked participants to share our recruitment information within their networks, adding 10 more participants through snowball sampling. We ensured balanced representation to prevent any single chain from dominating the sample's homogeneity. This method effectively captured diverse perspectives and was commonly used in previous research [46, 108, 114]. Potential participants contacted through snowball sampling also underwent screening, and all met the criteria. In total, 22 participants (12 parents and 10 teachers) took part in our study. Table 1 and 2 summarize the demographics of the participants.

| | Gender | Age | Occupation | | Gender | Age | Occupation |
|---|---|---|---|---|---|---|---|
| P01 | F | 38 | Teacher | P07 | F | 39 | Homemaker |
| P02 | F | 42 | Homemaker | P08 | F | 43 | Freelancer |
| P03 | F | 41 | Teacher | P09 | F | 32 | Homemaker |
| P04 | F | 35 | Homemaker | P10 | M | 43 | Management |
| P05 | F | 38 | Homemaker | P11 | F | 50 | Homemaker |
| P06 | M | 40 | Engineer | P12 | F | 37 | Sales |

**Table 1: Demographics of Parent Participants. P01-04, P06, P08, and P10 were directly recruited parent participants, and the others were snowball recruited.**

The demographic data of children raised by the interviewed parents are presented collectively in adherence to ethical guidelines. The children's ages ranged from 6 to 16 years, with 5 children between 6 and 10 years old and 7 between 11 and 16 years old. Their levels of ID varied, with 5 classified as mild, 4 as moderate, and 3 as severe. Additionally, 4 children were diagnosed with multiple disabilities, such as autism spectrum disorder and attention deficit hyperactivity disorder (ADHD) [38]. In terms of educational settings, 7 children attended special education schools, 3 attended inclusive education schools, and 2 were enrolled in rehabilitation centers. Their experience with mobile devices ranged from a few months to several years; specifically, 4 participants reported more

[1]https://www.theegg.com/social/china/xiaohongshu-red-chinas-rising-social-platform-impact-user-demographics-and-marketing-solutions/; https://www.demandsage.com/wechat-statistics/

than 3 years of experience, 5 had 2–3 years of experience, and 3 had 1–2 years of experience.

| | Gender | Age | Institution | Exp (yr) | | Gender | Age | Institution | Exp (yr) |
|---|---|---|---|---|---|---|---|---|---|
| T01 | F | 29 | Center | 6 | T06 | F | 28 | School | 5 |
| T02 | F | 24 | School | 3 | T07 | M | 26 | School | 3 |
| T03 | F | 25 | School | 3 | T08 | F | 32 | School | 6 |
| T04 | F | 25 | School | 2 | T09 | F | 23 | Center | 2 |
| T05 | F | 26 | Center | 4 | T10 | F | 40 | Center | 12 |

**Table 2: Demographics of Teacher Participants. The "Institution" column lists the organizations where they work: School" refers to special education schools, while "Center" refers to rehabilitation training centers. T01, T03, T04, T06, and T08 were directly recruited teacher participants, and the others were snowball recruited.**

## 4.4 Semi-structure Interview Procedure

Interviews were conducted between January and March 2025 via online meetings. Each interview lasted 45-60 minutes, and participants received a ¥100 honorarium. All interviewees understand that interviews will be recorded and their statements may be quoted anonymously in the final report. All data is considered confidential.

Our interviews with both parents and teachers focused on three parts: Firstly, for parental participants, we collected basic demographic data, including age and occupation, and examined their children's mobile device usage patterns, such as device ownership, primary usage purposes, frequently used functions or applications, and usage frequency. For teachers, we extended the demographic inquiry to include their observations of students' mobile device behaviors in educational settings, including estimated device ownership prevalence, daily usage patterns, and usage purposes. This aims to establish a basic understanding of the digital practice contexts involving parents and teachers.

Secondly, we explored the safety concerns parents and teachers hold regarding children's use of mobile devices. Through guided recall, participants were prompted to reflect on specific incidents that elicited unsafe, problematic operational behaviors demonstrated by children and perceived risk factors within device usage scenarios. This investigation facilitated the precise identification of root causes underlying the apprehensions of parents and teachers.

Finally, we explored how parents and teachers guide and educate children to use mobile devices safely, focusing on the measures and strategies they employ. Additionally, during the conversation, we intentionally asked parents and teachers to explain the connection between children's characteristics—such as cognitive abilities, social communication, and motor skills—and their use of strategies to manage digital safety risks. This approach helped us gain deeper insights into how specific student traits influence the effectiveness of different safety strategies.

The complete interview questions can be found in Appendix B.

## 4.5 Data Analysis

Given that all interviews were conducted in Mandarin, with participants' informed consent, we transcribed the recordings using an online tool[2], manually anonymized the transcripts to remove any identifying information, and then translated the anonymized text into English using Google Translate. Two researchers verified the accuracy and fidelity of the translations. Our methodology for analyzing these translated interview transcripts mainly involved the thematic analysis approach [41, 57]. The analysis process primarily encompassed the development and validation of the codebook, as well as the abstraction of core themes and conceptual frameworks.

**Generating initial codebook.** Initially, two researchers independently analyzed 20% of the interview transcripts to identify key safety issues perceived by parents and teachers of children with ID during mobile device use and the actions taken to mitigate these concerns. This process was also accompanied by coding of the scenarios mentioned by parents and teachers of children with ID using mobile devices, which provided the necessary background context for understanding the safety concerns and mitigation strategies better. The researchers then compared and discussed emerging themes. Discrepancies were thoroughly debated, and the themes were refined and synthesized into an initial codebook.

**Validating and completing codebook.** To validate the reliability of the codebook, we randomly selected another 10% of the interview transcripts for independent analysis by the two researchers. This resulted in a Cohen's Kappa score of $\kappa = 83.5$ [97], indicating high interrater reliability and mutual understanding of the codebook and its constituent themes.

After developing the initial codebook, both researchers independently coded the remaining 70% of the transcripts, meeting regularly after each 20% increment to ensure consistency. Disagreements prompted further inspection of the data, discussion about categories, and revisions to the scheme [48]. They discussed discrepancies and refined their interpretations, adding a code to the shared codebook only after reaching a mutual agreement.

This iterative process enhanced the rigor and validity of our findings. Data saturation was assessed by listing all emerging codes in the order of interviews (P01 to P12, and T01 to T10). Our analysis indicated that no new themes emerged in the later interviews, reinforcing our confidence that data saturation had been achieved.

**Developing themes and conceptual frameworks.** In this step, researchers created themes by organizing codes into meaningful groups and categories, transitioning from detailed codes to more abstract interpretations. Comprehensive association and analysis of these themes led to the development of conceptual frameworks for each RQ, resulting in unique data representations. Ultimately, five usage scenarios of mobile devices by children with ID were identified, which provide crucial context for understanding the digital safety risks faced by children with ID. Additionally, four core themes related to RQ1 were identified, and two key core themes were generated to answer RQ2.

As shown in Table 3, mobile devices are used by children with ID for entertainment, real-time communication, learning, payment, and life sharing. Among these, entertainment and real-time communication are the most frequently interacted scenarios.

Regarding RQ1, we identified four major concerns among parents and teachers: inappropriate imitation of harmful behaviors,

[2]https://www.feishu.cn/product/minutes

| Scenarios | Description |
|---|---|
| Entertainment | Engaging with low-age content in the form of short videos, stories, songs, and playing simple interactive games, for example, "BabyBus[3]". |
| Real-Time Communication | Engaging in audio and video calls, mainly with parents or close relatives. |
| Learning | Using educational tools such as children's reading apps and electronic picture books to learn phonetics, recognize characters, and understand basic concepts like identifying colors and objects. |
| Payment | Interacting with NFC and mobile payment systems. |
| Life Sharing | Posting photos or videos on social media. |

**Table 3: Mobile Devices Usage Scenarios by Children with ID. Children with ID use mobile devices for entertainment, real-time communication, learning, payment, and life sharing.**

misoperations causing financial loss, frauds such as scams or malicious contact, and cyberbullying rooted in the children's visible or behavioral differences. For RQ2, we categorized the strategies employed by parents and teachers into two main types: educational and technical management strategies. Educational strategies primarily include preventive guidance before using mobile devices and corrective constraints during and after use. Technical management strategies mainly involve setting functions and restrictions on mobile devices or utilizing support tools to isolate safety risks.

Two researchers were involved in this high-level generalization work, iteratively discussing and revising until reaching consensus on the frameworks. These frameworks encapsulate all the findings and insights from the data and serve to answer the RQs.

## 4.6 Limitation

Our study has identified two principal limitations: the regional homogeneity of our interviewees and the unbalanced gender representation among participants.

Firstly, all participants in this study are from China, which may limit the generalizability of the findings to other cultural contexts. We acknowledge and clarify the potential impact of this limitation on our results in the relevant sections (e.g., Section 7.1). However, the core elements under investigation—type of mobile devices, usage scenarios in the digital environment, general digital risks, and characteristics of children with ID—exhibit cross-cultural universality. Furthermore, given the insightful perspectives provided by the current respondents, this study could serve as a pilot study, informing future research across broader regions.

Secondly, our participant group shows a gender imbalance, with only three male samples. This aligns with two unavoidable realities: Children with ID may require round-the-clock care, which is more often provided by women who take on the role of homemakers[4], and the gender distribution in the field of special education tends to favor female educators [62, 141]. Although this may bias insights toward female perspectives, the current sample captures the practical experiences of the primary decision-makers, which does not significantly weaken the validity of our findings.

[4]https://en.wikipedia.org/wiki/Housewife

# 5 DIGITAL SAFETY CONCERNS FOR CHILDREN WITH ID (RQ1)

In this section, we focus on how parents and teachers perceive the safety risks associated with the use of mobile devices by children with ID. We elucidate on how these concerns arise and describe the perceived impacts as identified by parents and teachers. Table 4 shows the categorization of these perceived risks.

*Inappropriate imitation.* Our respondents are unanimously concerned that children with ID may encounter harmful content, such as pornography and violence, while using mobile devices for entertainment activities like video browsing and gaming, potentially leading to imitations. Among these concerns, the most concerning issue is the potential imitation of violent behavior.

The majority of our respondents indicated that their greatest concern is that children with ID might imitate violent behaviors and inflict them on others, exacerbating their social exclusion. For example, parents and teachers fear that children with ID might mistakenly associate violent and dangerous behaviors with "heroism" and "receiving rewards and attention", thereby exhibiting violent behaviors themselves. *"He watched a short video of PUBG: Battlegrounds[5], then used LEGO bricks as grenades to attack classmates and teachers"* (T04). Parents and teachers noted that these children, especially those receiving education in inclusive education schools, are already marginalized by their peers and even other parents and teachers, and they feared that imitating violent behavior would exacerbate this exclusion. *"His classmates already don't accept him much, and now he chases others around like in the game. He thinks it's fun, but others don't, so they don't play with him at all"* (P12).

Furthermore, over half of the interviewees expressed significant concerns regarding children with ID imitating inappropriate behaviors from pornographic content. This concern was particularly pronounced among parents of older children. Their primary apprehension centers on how cognitive impairments might lead these children to misinterpret suggestive language (e.g., "try it now") in adult videos or websites as instructional prompts. Distinct from typical worries about sexual cognitive distortions or addiction risks [26], respondents emphasized fears about public replication of such behaviors potentially causing social misunderstandings and exclusions. One parent recounted an incident where her near-adult child faced moral condemnation for unconscious self-exploratory behavior in public: *"She began touching her genitals in a restaurant - particularly awkward because she's physically adult-sized. I overheard bystanders making disparaging remarks"* (P11). Observers may misinterpret age-typical but inappropriate behavior as intentional misconduct rather than a manifestation of cognitive impairment.

*Unexpected misoperation.* Respondents believe that children with ID may unintentionally perform misoperations, leading to irreversible consequences, such as inadvertently triggering the "payment" function and causing financial loss or unintentionally dismissing risk prompts and directly entering risky environments.

Some interviewed parents are worried that when their children use their mobile phones, they may inadvertently activate some functions, posing a threat to property safety. Our respondents generally

[5]https://www.pubg.com/zh-cn/main

| Digital-Safety Concerns | Relevant Characteristics | Most Relevant Scenarios | Explanation |
|---|---|---|---|
| Inappropriate Imitation | Cognitive impairment; Social communication disorder | Entertainment | Concern that children with ID may imitate inappropriate or dangerous behaviors seen in videos or games, potentially leading to harm to themselves or others. |
| Unexpected Misoperation | Cognitive impairment; Motor coordination disorder; Speech and language delay | Payment | Children may accidentally trigger device functions—such as making purchases—due to limited understanding or poor motor control. |
| Fraud | Cognitive impairment; Speech and language delay | Real-Time Communication; Life Sharing | Children may fall victim in online fraud (e.g., telecom scam or grooming), especially due to difficulties with language comprehension and judgment. |
| Cyberbullying | Physical characteristics | Life Sharing | Children may be mocked or excluded online due to their appearance and behaviors, making them targets of cyberbullying. |

**Table 4: Perceived Digital Safety Risks for Children with ID in Mobile Device Use. This table summarizes the safety concerns identified by parents and teachers. The "Relevant Characteristics" column highlights traits of children with intellectual disabilities that may contribute to these risks or influence their digital behavior. The "Most Relevant Scenarios" column describes common contexts in which these risks are likely to occur during mobile device use.**

report that they have not provided dedicated phones for their children. Instead, children use their parents' phones with permission. However, parents typically do not implement additional settings or protective measures on the devices, as they consider themselves the primary and most frequent users. They find it cumbersome to repeatedly restrict and reopen access on a daily-use device. *"He may only use my phone for half an hour each day, but I have to set numerous restrictions and then readjust them when I use it myself. It's too cumbersome"* (P11). This shared device model introduces potential safety risks, as one parent reported that her child, while using her phone with the "password-free payment" function enabled, inadvertently clicked on a shopping app and placed an order for non-returnable items, resulting in financial loss. *"There was an expensive piece of jewelry in my shopping cart with no return policy. He placed the order, and I couldn't cancel it"* (P07).

Additionally, a few respondents expressed concern that children might not understand the actions occurring on device interfaces or might overlook on-screen security warnings, thereby placing themselves at risk. One teacher respondent shared her observations and perspective, noting that children with ID may be slow or unresponsive to complex navigation on mobile devices (e.g., switching between applications). They may not recognize the purpose of ongoing operations, making them prone to inadvertently activating buttons or functions. *"Many apps will display fancy advertising screens when opened and may even automatically jump to shopping apps. Children with ID respond very slowly, unable to understand what is happening, potentially resulting in unintentional clicks on purchase buttons"* (T04). Another teacher pointed out that beyond difficulties with device operations, they might not understand risk warnings on interfaces, clicking randomly and eventually entering risky websites. *"The webpage warns you that the URL you're about to click is risky, but the child doesn't understand this and keeps clicking the screen, eventually landing on a page with explicit ads"* (T03).

Moreover, respondents taking care of children with severe ID pointed out that these children exhibit marked motor impairments, which hinder their ability to perform fine motor tasks on screens. This limitation may inadvertently cause them to navigate to unintended interactive pages, thereby expanding potential risks and increasing the likelihood of accidental operations. *"Children with more severe conditions lack the fine motor control necessary for precise finger movements on interactive screens. Consequently, they may engage in random tapping, inadvertently triggering navigation to external pages"* (T08).

*Fraud.* Fraud involves criminal acts committed by attackers using online services and software to defraud or take advantage of victims [22, 32]. The interviewed parents and teachers primarily report concerns regarding exposure to telecom fraud under real-time communication scenarios, as well as risks associated with offline safety threats stemming from deceptive interactions when sharing content on social media platforms.

A few respondents are concerned that children with ID, due to their cognitive limitations and delayed language development, struggle to recognize malicious contacts online or understand the content of attacks, putting them at risk. Specifically, these respondents worry that children might receive scam calls during "real-time communication", easily trust the scammers, and install malicious software on their devices, leading to the leakage of critical passwords. *"They lack discernment, and I'm very worried they will follow to do"* (T07). In contrast, more respondents expressed the opposite view, believing that children with ID, due to communication barriers, might not even understand the intent of unfamiliar calls and thus fail to respond. *"They do not understand what's being said on the phone at all and just listen silently without responding"* (T03).

Additionally, a very small number of respondents mentioned concerns about the risks associated with social media platforms, even if children currently use them only for content sharing. For example, private messaging might lead to contact with strangers, and criminals could use fake event invitations to lure children into real-life meetings. Due to cognitive limitations, children may not recognize identity deception, and digital behaviors like location sharing and disclosing family information can create direct channels for crimes such as kidnapping, trafficking, and sexual assault. *"She uses TikTok, and I am very concerned that she might encounter fraud on the platform, which could lead to real-life harm"* (T04).

*Cyberbullying.* The interviewed parents and teachers are primarily concerned that children with ID might disclose unique physical

characteristics while sharing their lives on social platforms, leading to cyberbullying and resulting in social exclusion for both the children and their families. These children often exhibit distinctive physical features, such as facial characteristics associated with genetic conditions (e.g., Down syndrome), motor impairments due to muscle atrophy, or atypical behavioral patterns [70, 136].

More than half of the respondents expressed concerns that challenges related to the children's appearance or motor coordination, when shared through photos and videos on social media, might attract malicious scrutiny. While some respondents actively encourage children to document and share their lives, interpreting it as an expression of a positive and optimistic attitude, they are deeply worried that malicious users might transform the children's photos into mocking images or spread offensive comments in the comment sections, escalating into cyberbullying. Exacerbating the risk is the possibility that recommendation systems might inadvertently increase the exposure of such content, accelerating the widespread dissemination of harmful material. One parent noted: *"My child has distinctive facial features associated with Down syndrome. I am very worried that the videos he posts online might trigger cyberbullying, especially given the rapid spread of content online. I'm afraid that people around my child might join in the bullying"* (P11).

More seriously, respondents are concerned that such exclusion might affect the family's reputation. For instance, one parent reported that her colleagues saw the content her child shared on social media and subsequently mocked, defamed, and isolated her. *"They saw my child's video on TikTok and then spread rumors that I had given birth to an idiot. I also felt isolated"* (P12).

# 6 STRATEGIES FOR MITIGATING THE DIGITAL SAFETY CONCERNS (RQ2)

Our research also reveals various strategies parents and teachers adopt to address and prevent digital safety risks for children with ID. These strategies are categorized into two main types: educational strategies and technical management strategies, each detailed in Table 5. In the following sections, we clarify how parents and teachers implement these strategies to address their safety concerns.

## 6.1 Educational Strategies

Educational strategies are crucial measures used by parents and teachers to guide children in proactively avoiding digital safety risks. These strategies are detailed into two main categories: preventive guidance and corrective constraints. Specifically, preventive guidance includes methods such as scenario-based simulation, multi-sensory cueing, and gamified safety learning, which help children recognize or differentiate potential dangers before encountering risks. Corrective constraints, such as replacement behavior interventions and reinforcement and punishment techniques, are used to correct unsafe behaviors that have already occurred.

*6.1.1 Preventive Guidance.* To prevent children with ID from encountering safety crises and sustaining harm while using mobile devices for various activities, parents and teachers undertake a series of preventive efforts. These measures primarily include organizing scenario-based pretend play to simulate dangerous situations and train the responses of children with ID; providing multi-sensory cueing to help them evoke associative memory and form conditioned reflexes; and organizing gamified safety learning activities to make the learning process enjoyable and engaging, thereby enhancing their understanding and application of digital safety principles.

*Scenario-based simulation.* Scenario-based simulations involve replicating real-life situations, events, and activities [9, 137]. The interviewed parents and teachers believe that these activities can train the responses of children with ID to risks in a safe environment, thereby reinforcing their digital safety skills.

Some respondents indicated that due to difficulties with understanding and memory, children with ID often struggle to remember and clearly express what to do in dangerous situations, making it challenging to assess and measure their ability to respond to risks. Therefore, these respondents use scenario-based simulations to test and train children's responses to risks. They frequently organize scenario-based simulation activities, acting as malicious individuals online to simulate dangerous scenarios, to observe the children's reactions, and to test whether they have truly "remembered" the appropriate measures taught to them. For example, a parent might pretend to be a scammer or criminal, engaging in a simulated phone call to trick the child into revealing their home address, personal information, or opening the door. This helps expose unsafe behaviors, *"I pretended to be a delivery person on the call asking them to open the door, and they did"* (P02). Parents can then guide children towards correct safety practices and repeatedly test whether the child's behavior changes, *"I kept doing until they stopped opening the door, and only then did I feel they had truly remembered"* (P02).

While these interviewed parents and teachers consider scenario-based simulations an effective strategy for testing children's responses in safe risk environments, they also recognize its significant limitations. This strategy is typically based on limited scenarios, such as real-time communications, and is not easily adaptable to other fully interactive situations, like private messaging with strangers. Additionally, abstract concepts in the online environment hinder children's associations. For example, children may struggle to understand "what if you received a software installation package containing a virus?" As one parent mentioned, *"I can only use this method to train him what to do if he picks up and hears an unfamiliar voice. Beyond that, I feel like I can't simulate much more"* (P06).

*Multi-sensory cueing.* The multi-sensory cueing reinforces the memory of safety solutions through cross-modal inputs. The interviewed parents and teachers mainly design and apply tools that can stimulate sensory responses to help ID children establish multisensory associative memory mechanisms.

Due to cognitive limitations, children with ID often rely more on sensory learning. Respondents unanimously indicated that traditional methods relying solely on verbal instructions or written materials may be less effective for these children. Therefore, they depend on feedback mechanisms designed with visual cues, tactile feedback, and auditory signals to help children establish multisensory associative memory mechanisms [110, 128]. For example, one interviewed teacher reported using warning icon cards to provide visual cues, guiding children to recognize potential dangers through easily identifiable symbols. Specifically, when children navigate to an advertisement page, the teacher might use a red

| Cateogry | Specific Strategies with Label | | Explanation | Corresponded Concerns |
|---|---|---|---|---|
| Educational Strategies | Preventive Guidance | S01: Scenario-Based Simulation | Simulating real-life situations to help children practice appropriate responses—for example, parents pretending to be strangers calling their child. | Fraud |
| | | S02: Multi-Sensory Cueing | Using visual and tactile materials like icon cards to represent "dangerous links" or "safe websites", alongside cartoons and picture books to explain safety concepts. | Inappropriate Imitation; Fruad |
| | | S03: Gamified Safety Learning | Designing interactive games, such as quiz challenges and competitions, to teach safety knowledge through Q&A. | Fruad |
| | Corrective Constraints | S04: Replacement Behavior Intervention | Encouraging children to substitute unsafe behaviors with positive alternatives that meet the same needs or motivations. | Inappropriate Imitation |
| | | S05: Reinforcement and Punishment | Applying behavior management techniques, including rewards for safe behavior and penalties or withdrawal of privileges for unsafe actions. | Inappropriate Imitation; Fraud |
| Technical Management Strategies | S06: Functional Access Restriction | | Limiting/disabling device functions, such as blocking calls, filtering content, setting passwords, or disabling internet access. | Inappropriate Imitation; Unexpected Misoperation; Fraud; Cyberbulling |
| | S07: Technology-Based Control | | Using third-party apps or services, such as parental control software or built-in "kids mode" settings to monitor or guide usage. | Inappropriate Imitation; Unexpected Misoperation; Fraud; Cyberbulling |

**Table 5: Strategies of Parents and Teachers for Mitigating Digital Safety Concerns Among Children with ID. This table outlines two types of strategies used by parents and teachers: educational strategies and technical management strategies. Educational strategies include both preventive guidance, applied proactively to build safe habits, and corrective interventions, used to redirect inappropriate behaviors. Technical strategies focus on restricting device functionalities and leveraging supportive technologies to minimize digital risks. The last column illustrates the correspondence between strategies and concerns, where one strategy can address multiple safety concerns, and one safety concern can be managed by multiple strategies.**

exclamation mark to indicate potential risk. *"I made a large exclamation mark sign to train him to identify advertisement links. When a pop-up appears, I raise the sign to tell him it's an ad and not to click"* (T09). These safety cues are not fixed; rather, teachers adjust them based on each child's unique responses and preferences. For example, upon observing that a child is particularly sensitive to auditory stimuli, teacher may employ an alarm sound to signal safety risks when the child receives a call from an unknown number. *"Normally, she reacts with excitement upon hearing a sound; so when she receives a call from an unknown number, I used a small alarm to play a sound, telling her this is dangerous and she should reject it"* (T04).

*Gamified safety learning.* Gamified safety learning in teaching strategies involves incorporating game elements and mechanics into the digital safety education process to stimulate the learning interest and engagement of children with ID [45, 61]. The interviewed parents and teachers believed that this strategy leverages game elements such as challenges, points and rankings to make the teaching process more interesting and interactive, thereby stimulating children's interest in learning.

Some respondents, particularly teachers, reported using gamified activities to guide children with ID in addressing digital safety issues. For example, children can earn points by identifying safe and unsafe online behaviors, such as recognizing advertisement attempts and proposing countermeasures. Completing a series of safety challenges or consistently demonstrating safe online practices can earn them badges and raffle opportunities. *"I designed some game challenges related to recognizing the online content, dividing the children into two teams for a points competition"* (T07). Respondents believe this is an engaging approach, as they observed that integrating these game elements significantly increased children's engagement. The children were more likely to participate and remember the information. *"I asked questions after the game, and I found that their feedback was more positive in this way, and they seemed to remember more"* (T07).

*6.1.2 Corrective Constraints.* Corrective constraints are strategies employed by parents and teachers upon observing behaviors in children with ID that are detrimental to digital safety practices. Two types of these strategies emerged from our findings: replacement behavior intervention as well as reinforcement and punishment.

*Replacement behavior intervention.* Replacement behavior intervention is a supportive strategy based on the analysis of behavioral motivations [98]. Its core logic lies in uncovering the motivations of problematic behaviors through functional behavior assessment and subsequently introducing healthier behavior patterns that serve the same function to achieve behavior reshaping [99].

Our respondents frequently mentioned this approach when addressing the issue of children encountering unhealthy and harmful online content. As one interviewed teacher reported, she observed that children might come across "thirst trap[6]" videos during

[6]A thirst trap is a type of social media post intended to entice viewers sexually. https://en.wikipedia.org/wiki/Thirst_trap

entertainment activities, where the strong rhythm and auditory stimulation from the actions and music make them want to keep watching. In such cases, she applies the principle of "equivalent functional replacement", selecting alternatives that both satisfy the child's original motivation and accommodate their personal interests, thereby fostering healthier substitute behaviors. For example, she chooses fitness videos as an alternative medium—these videos not only include regular physical movements and dynamic effects from rhythmic background music (satisfying the initial motivation) but also respect the child's affinity for music and dance. *"He gets very excited and starts jumping when he sees such videos, since he loves music and rhythm, we found many fitness videos featuring very fit instructors to engage him in exercise"* (T02). For children with ID, this replacement intervention is particularly effective because their limited understanding may prevent them from grasping the meaning of the replaced behavior, making them more likely to accept the alternative medium. *"In fact, he doesn't understand what inappropriate content is or the sexual implications; he is simply attracted by the rhythm and dance movements, so using fitness videos as a replacement is a logic he easily accepts"* (T02).

*Reinforcement and punishment.* Reinforcement and punishment are key strategies within Applied Behavior Analysis (ABA) [130]. Reinforcement, which can be positive or negative, aims to increase the occurrence of target behaviors. Positive reinforcement involves giving rewards or praise after a behavior [140], while negative reinforcement involves removing an aversive stimulus, such as lifting restrictions on entertainment time [35]. Punishment, on the other hand, aims to decrease problematic behaviors by applying an aversive stimulus [94, 146], such as assigning extra chores.

Among these strategies, our respondents most commonly use positive reinforcement and punishment to manage children's digital safety practices. Specifically, in the application of positive reinforcement, parents and teachers reward children with stickers or snacks that the children like when they perform actions that help avoid digital risks, such as immediately closing pop-up ads. *"She loves Hello Kitty, so I bought many stickers to give her when she does the right thing"* (P09). In addition, they usually use punishment measures (eg, standing in the corner) to deal with children's wrong practices, such as randomly downloading apps that jump to the App Store. *"Appropriate physical punishment makes him aware of the consequences of his actions"* (P03). The reason for combining positive reinforcement and punishment is that parents and teachers do not want a single strategy to lead to bargaining or rebellious behavior in children, thus, they tend to use mixed strategies more frequently.

## 6.2 Technical Management Strategies

In addition to guiding children through educational strategies, parents and teachers sometimes directly implement technical management strategies to manage mobile devices. On one hand, they enforce certain functional access restrictions on the devices; on the other hand, they utilize technology-based controls to manage and control their children's digital environments.

*Functional access restriction.* Functional access restrictions refer to implementing a series of isolation settings on mobile devices to prevent children from encountering potential risks.

Among all respondents, nearly all interviewed parents reported using this measure. The measures they typically adopt include restricting device usage, internet access, limiting the installation of high-risk applications, and disabling payment functions to prevent children from inadvertently entering dangerous areas due to a lack of judgment. Respondents unanimously believe that such strict restrictions eliminate the opportunity for children to encounter risks, thereby directly mitigating safety hazards. *"If he can't access it, then these problems don't exist"* (P04). Additionally, parents often incorporate filtering and relative restrictions as part of their strategy. For example, using the "not interested" feature to filter recommendations related to pornography, violence, and gore in applications and using call-blocking features to filter unknown numbers are classic strategies reported by respondents. Furthermore, parents regularly monitor and adjust these settings to ensure that these protective measures remain effective as their children's digital habits evolve.

One important reason for implementing this strategy is that respondents sometimes struggle to explain potential risks or what the "things" that cause safety risks are, such as being unable to describe and explain what a "phishing link" is. Therefore, they choose games that do not require internet connectivity to ensure the application does not redirect to pages that might contain phishing links, keeping the child unaware of the existence of such things. *"I have restricted these things, so he doesn't even know they exist"* (P01). Furthermore, a underlying reason is that these measures may be implemented to avoid inconvenience or safeguard the caregivers' own interests. For example, disabling payment functions seems more focused on protecting caregiver asset security than on promoting the children's own interests, a neglect that we address in the Discussion.

*Technology-based controls.* Technology-based controls primarily involve the use of additional technological tools to control, monitor, and manage the digital environment of children, typically including the utilization of remote control tools and relying on the kids modes.

A few respondents, particularly parents, mentioned "parental control apps", which enable them to monitor and supervise their children's activities on devices in real-time, as well as remotely control and lock mobile devices. This provides parents with a greater sense of control, thereby offering psychological reassurance. *"I can see which app he is using, and I can directly close the app he is using or even shut down the mobile device from my phone"* (P08).

Additionally, more than half of the respondents indicated that they use "kids mode" to control the content their children can access. These respondents stated that applications with the kids mode ensure that the browsing content aligns with the children's cognitive and developmental levels, filtering out inappropriate content to provide a healthy and safe online environment. Particularly, the kids mode often pushes more lower-age content for children, which better meets the needs of children with ID. *"Applications under kids mode are all for cartoon-based content, with nothing unsafe"* (P01).

# 7 DISCUSSION

Our research investigates the perceptions and strategies of parents and teachers in addressing the safety risks associated with mobile device use by children with ID. Based on our findings, this section first compares the digital safety concerns expressed by parents and

teachers for children with ID to those for typically developing children, identifying similarities and unique aspects of these concerns. Then, we discuss the challenges faced in implementing digital safety strategies in special education, highlighting key considerations for optimizing current digital safety paradigms. Finally, we propose methods to enhance the safety of vulnerable groups by optimizing existing systems as well as introducing new solutions to support the implementation of digital safety education.

## 7.1 Similarity and Uniqueness of Perceived Digital Safety Concerns

As clarified in Section 5, parents and teachers identified four primary digital safety concerns for children with ID: inappropriate imitation, unexpected misoperations, fraud, and cyberbullying. While these concerns appear similar to those raised for typically developing children, our analysis reveals meaningful differences in how these risks are perceived and experienced in the context of ID.

To examine these distinctions, we adopt a risk management framework [11] that categorizes risk into three components: risk factors (what triggers a risk), risk events (how the risk manifests), and risk consequences (resulting harm). This framework allows us to distinguish between digital risks shared across populations and those specific to the vulnerabilities of children with ID.

*Shared risk types, distinct risk mechanisms.* Many digital safety concerns—such as exposure to harmful content, online contact with strangers, and cyberbullying [42]—are not unique to children with ID. These are objective risks arising from external digital environments and are common across various user groups. Prior research captures these under the well-established "3Cs" model: content, contact, and conduct risks [82]. The concerns raised in our study align with this model: inappropriate imitation relates to harmful content, frauds reflect dangerous contact, and cyberbullying stems from online conduct. These shared risk types indicate that children with ID, like their peers, are exposed to digital dangers shaped by the design and openness of online systems.

However, what distinguishes the experiences of children with ID is how these risks are triggered. In this regard, our findings highlight the importance of subjective risk factors, which are rooted in the child's internal capacities—such as cognitive limitations, speech and language delays, and motor coordination issues. These subjective factors do not create new categories of risk but alter the likelihood and manner in which risks are encountered. For instance, an advertisement with a hidden phishing link may pose a threat to many users, but a child with ID may be more likely to click on it impulsively due to sensory-seeking or difficulty interpreting interface cues [73]. Similarly, accidental misoperations may affect other groups—like elderly or visually impaired users—but the underlying mechanisms differ: for children with ID, the cause may be cognitive immaturity, whereas for elderly it may stem from cognitive decline, and for visually impaired users, a lack of visual feedback [105, 135]. Thus, risk types can be shared, but risk triggers are group-specific and shaped by developmental or functional profiles.

*Emphasis on basic, sensory-driven risk events.* Another distinction in the perceived concerns of parents and teachers of children with ID lies in the simplicity and sensory immediacy of the risk events. While prior studies on typically developing children often focus on sophisticated threats—such as identity fraud or long-term manipulation [52, 67]—parents and teachers of children with ID express more concern about basic, easily-triggered events, such as clicking a misleading button or imitating a behavior shown in a cartoon (refer to Section 5). These events are often driven by visual appeal, impulsivity, or literal interpretation, which are common among children with ID [53]. This pattern suggests that for this group, risk management must prioritize low-level triggers—especially those embedded in design elements that exploit sensory salience.

This insight may also apply to other populations with similar sensory or cognitive processing profiles, including children with ADHD, reading difficulties, or autism spectrum disorder [16, 28, 64]. In these cases, accessible design and reduced sensory overload are not merely usability enhancements but critical safety mechanisms.

*Social exclusion as the central consequence.* The final distinction lies in the perceived consequences of digital risks. While existing literature on typically developing children links digital threats to outcomes like anxiety, depression [56], behavioral dysregulation [83], or cognitive distortions [80], parents and teachers of children with ID place the greatest emphasis on social exclusion. This concern reflects both the pre-existing social vulnerabilities of this group and the fear that inappropriate digital behavior—such as imitating violent or sexualized content—may further isolate them (as mentioned in Section 5). For children with limited social awareness or communicative ability, even small incidents can escalate into reputational harm or peer rejection, especially in inclusive education environments.

Importantly, the impact of digital exclusion often extends beyond the child. Some parents reported that posting photos or videos of their children online—even in seemingly positive contexts—led to ridicule or discriminatory comments targeting both the child and their family (refer to Section 5). This experience of online stigma reinforces social marginalization and may discourage families from engaging in digital spaces altogether. While we acknowledge that cultural contexts shape respondents' perspectives to some extent — for instance, in China, the act of "sharenting (known as shaiwa in China)" on social media carries implications of familial resource demonstration rather than constituting mere personal sharing [150] — parents may exhibit heightened sensitivity to critical comments on shared content. But in fact, this also reflects that digital risk is not only a technical or behavioral issue but a social one, tied closely to community norms and public perception.

Therefore, addressing the digital safety of children with ID requires not only protective features but also systems that foster positive social representation and inclusion. Designing safer digital environments for vulnerable users must extend beyond filtering content to prioritize dignity, empathy, and participation.

## 7.2 Challenges in Implementing Digital Safety Strategies

Our findings reveal that parents and teachers rely primarily on two strategies: educational strategies and technical management strategies. While both approaches show initiative on the part of

parents and teachers, they are constrained by significant structural challenges—particularly the individualization and fragmentation of educational strategies and the applicability of technological management strategies in terms of cognitive accessibility.

*7.2.1 Challenge of individualization and fragmentation in educational strategies.* In our research, most parents and teachers prefer to begin with educational strategies. As seen in Section 6, they employ techniques such as scenario-based simulations, multi-sensory cueing, and gamified learning activities (S01–S03) to help children understand what online risks are and how to respond. Additionally, they implement alternative behavior interventions and reinforcement and punishment (S04, S05) to manage children's unsafe behaviors in digital environments. These approaches are often tailored to the child's cognitive profile and daily experiences, which makes them accessible on a personal level.

However, the effectiveness of these methods is limited by their high dependence on parents' and teachers' resources and expertise. Parents often develop their own tools through trial and error, while teachers lack access to standardized lesson plans or interdisciplinary support (e.g., integrating digital literacy with special education). This makes educational efforts fragmented and non-transferable, with success depending more on the parents' and teachers' creativity than on any formalized system.

This pattern is echoed in studies of other disability groups. For example, parents of children with language impairments or dyslexia also report difficulty accessing safety materials or clear teaching guidelines [27, 49]. These cases reveal a recurring structural issue: Parents and teachers are expected to manage digital safety without systems or guidance designed to help them do so. In summary, while educational strategies are conceptually sound, they lack systemic backing and are not scalable.

*7.2.2 Challenge of cognitive mismatch in technical management strategies.* When educational efforts are insufficient, parents and teachers turn to technical management strategies (S06–S07). These include forced isolation restrictions such as uninstalling apps and disabling internet access, as well as control and management through remote monitoring and kids mode features. While these strategies mitigate risks, on one hand, restrictions from parents and teachers on technology, devices, and functions may limit the cognitive empowerment opportunities that mobile devices can provide to children. On the other hand, although current technical tools are designed with safety in mind, they do not consider how to dynamically adapt to and support children's cognitive development needs while enhancing safety measures.

*Mismatch caused by restrictive strategies of parents and teachers.* Our findings indicate that parents and teachers perceive technical management strategies, particularly functionality restrictions, as a fallback mechanism when educational strategies encounter obstacles. Unlike parents and teachers of typically developing children, who keep technology restrictions within reasonable limits—such as setting up network proxies to allow supervised digital interactions and granting children some autonomy [25, 42]—parents and teachers of children with ID often adopt stricter technical management strategies. These include uninstalling apps, enabling kids mode, or even disabling network access.

However, while these practices may mitigate risk factors to some extent and provide psychological comfort to parents and teachers, they may also sever children's connection to cognitive development resources in the digital age. This restriction limits opportunities for children to cultivate digital literacy, social adaptability, and autonomous learning through controlled online interactions. For instance, disabling payment functions might hinder children's understanding of numbers, money, and basic payment skills, potentially exacerbating cognitive isolation and creating a mismatch with the developmental needs of children in a digital society.

More importantly, these practices neglect children's preferences and needs, leaving them as passive recipients of imposed strategies. Grounded in the principles of disability justice [12] and the "Nothing About Us Without Us" guideline by WHO [95], we advocate for greater inclusion of the voices of children with ID. Accordingly, schools and welfare organizations should organize additional mobile device–related activities that enable children to engage in direct dialogue and alternative forms of expression—such as drawing [74], singing [133], building blocks [23], and sandplay therapy [131]—to articulate their needs and emotions. Moreover, government agencies should strengthen their oversight to ensure these initiatives prioritize children's welfare. We also call upon developers and educators in the subsequent design recommendations to collaboratively construct the human-centered digital safety solutions that balance safety protection and cognitive development. These solutions aim to promote a digital environment that is both secure and accessible, ensuring that protective measures do not inadvertently hinder opportunities for learning, autonomy, and growth.

*Mismatch caused by technology rigidity.* In addition to the mandatory restrictions, parents and teachers also rely on technological tools to manage children's digital environments and safety risks, such as remote monitoring tools or enabling kids mode. While these tools provide safety solutions and help reduce risks in the short term—especially when children's self-regulation abilities are limited—their design often fails to consider how to match children's cognitive needs and provide ongoing support as they develop.

For example, remote monitoring applications may be suitable for the early stages of child development, allowing parents and teachers to monitor and control children's real-time online activities. However, as children grow older, the use of these tools may conflict with their privacy awareness. Additionally, these tools often involve parents remotely controlling devices, which can confuse or frustrate children with ID who may not understand system feedback or why certain functions are restricted. Similarly, kids mode typically features low-age cartoon content, which, while visually suitable for children with ID [142], may lack the content value needed to enhance cognitive development and social integration.

These examples illustrate that mainstream digital safety tools often lack cognitive adaptability, meaning they cannot protect users while simultaneously adapting to and supporting their evolving needs—a fundamental requirement for any developmental user group. Therefore, a paradigm shift in digital safety design should be considered—from expecting users to adhere to rigid tool logic to designing systems that actively support contextual understanding and progressive skill development.

## 7.3 Design Implications

Based on our understanding of the current digital safety practices for children with ID, this section proposes two primary directions for improving digital safety practices for children with ID: optimizing the usability of current device systems and recommendation algorithms, and developing perceptible, simulation-based educational tools that align with the learning needs of children with ID in special education contexts.

*Optimizing safety mechanisms in existing systems.* Several improvements to existing digital safety systems could significantly enhance their usability for children with ID. First, current risk alerts largely rely on textual prompts, which—as illustrated in Section 5—are often ineffective for children with ID who rely on sensory stimulation for information [58]. To address this, safety systems should adopt multimodal alert methods that combine auditory, visual, and tactile cues—a strategy that may also benefit individuals with reading difficulties, older adults, and the visually impaired [3, 109]. Furthermore, given that children with ID exhibit deficits in information processing and command comprehension [134], it is advisable to employ familiar voices and personally meaningful cues instead of generic signals [81]. To this end, caregivers should be empowered to personalize these alerts by recording custom sounds using voices and phrases familiar to the child. Additionally, considering the slower rate at which these children adopt new information and their generally lower memory retention and learning speed [123], risk alerts can be repeated as nursery rhymes, and cartoon characters familiar to the children can be introduced as system companions to guide them in reinforcing safety practices.

Second, content recommendation and review mechanisms require meaningful reconfiguration. As highlighted in Sections 5 and 7.1, social exclusion is a central concern for parents and teachers of children with ID. Yet, current recommendation algorithms are often socially biased and not designed to prevent reputational or relational harm. We suggest implementing a "vulnerable group protection mode" that disables certain social discovery features—such as "people you may know"—and instead promotes a weak social association model. Prioritizing content from interest-based communities (e.g., special education, inclusive design) over acquaintance-based suggestions could help reduce exposure to social judgment or bullying. Additionally, platforms should establish "inclusive content review guidelines" that upgrade offensive expressions like "you are so dumb" to high-risk flags when used in ID-related contexts. Moderation algorithms should be trained to distinguish between casual language and structurally discriminatory speech, thus offering more effective protection against online reputational harm. These refinements would also serve other marginalized groups, such as LGBTQ+ users and ethnic minorities, who face similar risks in algorithmic environments [15, 71].

Third, mobile device operating systems should better accommodate family-sharing scenarios common in households with children with ID. As noted in Section 5, many parents allow their children to use their phones because manually switching between restrictions is cumbersome. To address this, devices could implement user-sensitive modes that automatically adjust system settings upon recognizing a child user—whether through facial recognition, voice input, or other biometric indicators. It is important to note that the collection and use of children's biometric data are subject to regional regulations. For instance, in China, reasonable use is allowed with parental consent and appropriate legal supervision[7]. We also acknowledge the inherent privacy concerns of biometric solutions. Therefore, in addition to biometric options, we recommend a universal mode-switching mechanism that allows parents to instantly toggle the entire system. For example, switching to "kids mode" would not only alter system settings but also automatically activate all child-specific configurations across installed applications. This one-touch solution minimizes caregiver effort while ensuring uniform safety preferences. Furthermore, the front-end design of kids mode should be as simple and conspicuous as possible, avoiding complex function buttons—an important consideration since children with ID often struggle with fine motor coordination, leading to inadvertent activations (as mentioned in Section 5).

Finally, current parental control applications should be optimized to better meet the practical needs of children with ID and their parents. Our findings indicate that parents often use these controls solely to disable apps, but children's limited cognitive abilities may hinder their understanding of sudden restrictions. This can lead to confusion, frustration, or even resistance to digital engagement, as discussed in Section 7.2.2. To support, we recommend reconfiguring parental controls into an accompanied guidance system. Instead of shutting down applications and devices upon detecting risky behavior, the system should initiate a real-time dialogue between parent and child. This conversation would help uncover the child's underlying motivations while gently guiding them toward safer practices. Moreover, the parental interface should incorporate structured communication tools—such as contextual dialogue prompts developed by educators and psychologists—to facilitate constructive and empathetic discussions.

*Developing simulation-based safety education tools.* A core challenge in promoting digital safety for children with ID is that traditional methods—especially verbal explanations or rule-based instruction—are often ineffective in helping them recognize abstract threats. As shown in Section 6, parents and teachers frequently use behavioral interventions or simplified cues, indicating a need for more engaging and cognitively accessible teaching tools.

To address this, we propose the development of scenario-based simulation trainers that allow children to rehearse responses to digital safety risks in controlled, interactive environments. Unlike passive teaching methods or caregiver-led simulations, these trainers would combine virtual reality or interactive media with multi-sensory feedback, offering more immersive and memorable learning experiences. For example, a simulated environment could replicate the experience of receiving a suspicious message or encountering a misleading advertisement, guiding the child step-by-step through appropriate reactions. Additionally, it is important to design progressive training modes, such as developing a series of scenario stories and graded difficulty levels for simulation tasks. This approach would complement the current safety education measures by addressing the challenges of fragmentation and lack of systematic guidance, as discussed in Section 7.2.2.

[7] https://personalinformationprotectionlaw.com/PIPL/hello-world/

This approach draws on previous studies demonstrating the effectiveness of virtual simulations in special education, which have been used to teach skills such as environmental navigation, social interaction, and basic life tasks [78, 116]. However, few existing tools apply these principles specifically to digital safety contexts. By integrating gamification elements—such as badges, challenges, and rewards—alongside animations and audio-visual prompts, children with ID can build behavioral memory through repetition, positive reinforcement, and emotional engagement. These simulation tools would extend the "scenario-based simulations" already practiced by parents and teachers (see Section 6.1.1), but with greater consistency, scalability, and pedagogical depth.

Additionally, the use of animated narratives and character-based storytelling can help explain abstract concepts—such as scams, privacy, or digital manipulation—in ways that align with children's cognitive frameworks. Such tools could be deployed in both school and home environments, providing valuable supplementary resources for parents and teachers and helping institutionalize digital safety education within special education systems.

## 8 CONCLUSION

This study focuses on the digital safety challenges faced by children with ID and the mitigation strategies employed by their parents and teachers. The findings indicate that children with ID are more vulnerable in digital environments due to their limited cognitive and adaptive abilities. Parents and teachers are particularly concerned about the risks associated with sensory stimuli and social exclusion. Additionally, we found that parents and teachers typically address digital safety issues through a combination of proactive education and technical mediation. However, they face challenges such as fragmented educational strategies and ambiguous boundaries in technological control. These insights collectively highlight the limitations of generic solutions and provide valuable references for optimizing safety mechanisms in existing systems and developing new educational tools, enabling this vulnerable group to safely and effectively explore the complex digital world.

## REFERENCES


[1] 2025. The Belmont Report - Ethical Principles and Guidelines for the Protection of Human Subjects of Research. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html

[2] Tousif Ahmed, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. 2016. Addressing physical safety, security, and privacy for people with visual impairments. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 341–354.

[3] Fahad Alanazi, Karen Renaud, and Irina Tal. 2023. Understanding the impact of dyslexia on online privacy and security. In *2023 Cyber Research Conference-Ireland (Cyber-RCI)*. IEEE, 1–7.

[4] Monica Anderson. 2018. A majority of teens have experienced some form of cyberbullying. (2018).

[5] Arnav Arora, Preslav Nakov, Momchil Hardalov, Sheikh Muhammad Sarwar, Vibha Nayak, Yoan Dinkov, Dimitrina Zlatkova, Kyle Dent, Ameya Bhatawdekar, Guillaume Bouchard, et al. 2023. Detecting harmful content on online platforms: what platforms need vs. where research efforts go. *Comput. Surveys* 56, 3 (2023), 1–17.

[6] Priti Arun and Shikha Jain. 2022. Use of smart phone among students with intellectual and developmental disability. *Journal of Psychosocial Rehabilitation and Mental Health* 9, 4 (2022), 447–452.

[7] Karla Badillo-Urquiola, Xinru Page, and Pamela J Wisniewski. 2019. Risk vs. restriction: The tension between providing a sense of normalcy and keeping foster teens safe online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–14.

[8] Shaowen Bardzell and Jeffrey Bardzell. 2011. Towards a feminist HCI methodology: social science, feminism, and HCI. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 675–684.

[9] Erin E Barton and Mark Wolery. 2008. Teaching pretend play to children with disabilities: A review of the literature. *Topics in Early Childhood Special Education* 28, 2 (2008), 109–125.

[10] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, et al. 2024. Sok: Safer digital-safety research involving at-risk users. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 635–654.

[11] Heinz-Peter Berg. 2010. Risk management: procedures, methods and experiences. *Reliability: Theory & Applications* 5, 2 (17) (2010), 79–95.

[12] Patricia Berne, Aurora Levins Morales, David Langstaff, and Sins Invalid. 2018. Ten principles of disability justice. *WSQ: Women's Studies Quarterly* 46, 1 (2018), 227–230.

[13] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M Redmiles, and Angelika Strohmayer. 2022. Ethical practices for security research with at-risk populations. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 546–553.

[14] Lindsay Blackwell, Jill Dimond, Sarita Schoenebeck, and Cliff Lampe. 2017. Classification and its consequences for online harassment: Design insights from heartmob. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–19.

[15] Ana-Maria Bliuc, Nicholas Faulkner, Andrew Jakubowicz, and Craig McGarty. 2018. Online networks of racial hate: A systematic review of 10 years of research on cyber-racism. *Computers in Human Behavior* 87 (2018), 75–86.

[16] Martin Bøg, Jens Dietrichson, and Anna A Isaksson. 2021. A multi-sensory tutoring program for students at risk of reading difficulties: Evidence from a randomized field experiment. *The Journal of Educational Research* 114, 3 (2021), 233–251.

[17] Brian Bourke. 2014. Positionality: Reflecting on the research process. *The qualitative report* 19, 33 (2014), 1–9.

[18] Danah Boyd and Eszter Hargittai. 2013. Connected and concerned: Variation in parents' online safety concerns. *Policy & Internet* 5, 3 (2013), 245–269.

[19] Elena Bozzola, Giulia Spina, Margherita Ruggiero, Luigi Memo, Rino Agostiniani, Mauro Bozzola, Giovanni Corsello, and Alberto Villani. 2018. Media devices in pre-school children: the recommendations of the Italian pediatric society. *Italian journal of pediatrics* 44 (2018), 1–5.

[20] Gary Bunch* and Angela Valeo. 2004. Student attitudes toward peers with disabilities in inclusive and special education schools. *Disability & Society* 19, 1 (2004), 61–76.

[21] Colin Burke and Cinnamon Bloss. 2020. Social media surveillance in schools: rethinking public health interventions in the digital age. *Journal of medical internet research* 22, 11 (2020), e22612.

[22] Mark Button, Carol McNaughton Nicholls, Jane Kerr, and Rachael Owen. 2014. Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand journal of criminology* 47, 3 (2014), 391–408.

[23] Zhenyao Cai. 2023. EmotionBlock: A Tangible Toolkit for Social-emotional Learning Through Storytelling. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference*. 693–696.

[24] Joanne Cantwell, Orla Muldoon, and Stephen Gallagher. 2015. The influence of self-esteem and social support on the relationship between stigma and depressive symptomology in parents caring for children with intellectual disabilities. *Journal of Intellectual Disability Research* 59, 10 (2015), 948–957.

[25] Jiaxun Cao, Anupam Das, Pardis Emami-Naeini, et al. 2024. Understanding parents' perceptions and practices toward children's security and privacy in virtual reality. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1554–1572.

[26] Patrick J Carnes. 2001. Cybersex, courtship, and escalating arousal: Factors in addictive sexual desire. *Sexual Addiction & Compulsivity* 8, 1 (2001), 45–78.

[27] Sue Caton and Roderick Landman. 2022. Internet safety, online radicalisation and young people with learning disabilities. *British Journal of Learning Disabilities* 50, 1 (2022), 88–97.

[28] Zaira Cattaneo, Tomaso Vecchi, Cesare Cornoldi, Irene Mammarella, Daniela Bonino, Emiliano Ricciardi, and Pietro Pietrini. 2008. Imagery and spatial processes in blindness and visual impairment. *Neuroscience & Biobehavioral Reviews* 32, 8 (2008), 1346–1360.

[29] Darren David Chadwick. 2019. Online risk for people with intellectual disabilities. *Tizard Learning Disability Review* 24, 4 (2019), 180–187.

[30] Lisa Chelkowski, Zheng Yan, and Kristie Asaro-Saddler. 2019. The use of mobile devices with students with disabilities: A literature review. *Preventing School Failure: Alternative Education for Children and Youth* 63, 3 (2019), 277–295.

[31] Sharon Lynn Chu, Brittany Garcia, and Beth Nam. 2019. Understanding context in children's use of smartwatches for everyday science reflections. In *Proceedings of the 18th ACM international conference on interaction design and children*. 83–93.

[32] Cassandra Cross. 2019. Online fraud. *Oxford research encyclopedia of criminology* (2019), 1–32.

[33] John-Joe Dawson-Squibb, Eugene Lee Davids, Marisa Viljoen, Kirsty Rice, and Dan J Stein. 2023. The WHO international classification of diseases 11th revision (ICD-11). In *Handbook of clinical child psychology: Integrating theory and research into practice*. Springer, 53–78.

[34] Marie-Catherine De Marneffe, Bill MacCartney, Christopher D Manning, et al. 2006. Generating typed dependency parses from phrase structure parses.. In *Lrec*, Vol. 6. 449–454.

[35] Diane ED Deitz and Alan C Repp. 1983. Reducing behavior through reinforcement. *Exceptional Education Quarterly* 3, 4 (1983), 34–46.

[36] Dominic DiFranzo, Yoon Hyung Choi, Amanda Purington, Jessie G Taft, Janis Whitlock, and Natalya N Bazarova. 2019. Social media testdrive: Real-world social media education for the next generation. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–11.

[37] Meltem Dinleyici, Kursat Bora Carman, Emel Ozturk, Figen Sahin-Dagli, et al. 2016. Media use by children, and parents' views on children's media usage. *Interactive journal of medical research* 5, 2 (2016), e5668.

[38] June E Downing. 1996. Including students with severe and multiple disabilities in typical classrooms: Practical strategies for teachers. (1996).

[39] Aiman El Asam and Adrienne Katz. 2018. Vulnerable young people and their experience of online risks. *Human–Computer Interaction* 33, 4 (2018), 281–304.

[40] Lidia F Fatikhova and Elena F Sayfutdiyarova. 2016. Understanding of unsafe situations by children with intellectual disabilities. *Psychology in Russia* 9, 4 (2016), 62.

[41] Jennifer Fereday and Eimear Muir-Cochrane. 2006. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International journal of qualitative methods* 5, 1 (2006), 80–92.

[42] Diana Freed, Natalie N Bazarova, Sunny Consolvo, Eunice J Han, Patrick Gage Kelley, Kurt Thomas, and Dan Cosley. 2023. Understanding digital-safety experiences of youth in the US. In *Proceedings of the 2023 CHI Conference on Human factors in computing Systems*. 1–15.

[43] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. " Is My Phone Hacked?" Analyzing Clinical Computer Security Interventions With Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[44] Nenad Glumbić, Branislav Brojčin, Mirjana Đorđević, and Vesna Žunić-Pavlović. 2021. Characteristics of mobile phone use in adolescents identified with mild intellectual disability who attend special schools in Serbia and their non-disabled peers in mainstream schools. *British Journal of Learning Disabilities* 49, 2 (2021), 217–229.

[45] Daniel Gooch, Asimina Vasalou, Laura Benton, and Rilla Khaled. 2016. Using gamification to motivate students with dyslexia. In *Proceedings of the 2016 CHI Conference on human factors in computing systems*. 969–980.

[46] Leo A Goodman. 1961. Snowball sampling. *The annals of mathematical statistics* (1961), 148–170.

[47] Foad Hamidi, Morgan Klaus Scheuerman, and Stacy M Branham. 2018. Gender recognition or gender reductionism? The social implications of embedded gender recognition systems. In *Proceedings of the 2018 chi conference on human factors in computing systems*. 1–13.

[48] David Hammer and Leema K Berland. 2014. Confusing claims for data: A critique of common practices for presenting qualitative research on learning. *Journal of the Learning Sciences* 23, 1 (2014), 37–46.

[49] Sophie Harding, Maya Chauhan-Sims, Emily Oxley, and Hannah M Nash. 2023. A Delphi study exploring the barriers to dyslexia diagnosis and support: A parent's perspective. *Dyslexia* 29, 3 (2023), 162–178.

[50] E Hartman, S Houwen, E Scherder, and C Visscher. 2010. On the relationship between motor performance and executive functioning in children with intellectual disabilities. *Journal of Intellectual Disability Research* 54, 5 (2010), 468–477.

[51] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*. 105–122.

[52] Beatrice Hayes, Alana James, Ravinder Barn, and Dawn Watling. 2022. "The world we live in now": A qualitative investigation into parents', teachers', and children's perceptions of social networking site use. *British Journal of Educational Psychology* 92, 1 (2022), 340–363.

[53] Erin A Hayes, Catherine M Warrier, Trent G Nicol, Steven G Zecker, and Nina Kraus. 2003. Neural plasticity following auditory training in children with learning problems. *Clinical neurophysiology* 114, 4 (2003), 673–684.

[54] Ellen Johanna Helsper and David Smahel. 2020. Excessive internet use by young Europeans: psychological vulnerability and digital literacy? *Information, communication & society* 23, 9 (2020), 1255–1273.

[55] Christothea Herodotou. 2018. Young children and tablets: A systematic review of effects on learning and development. *Journal of Computer Assisted Learning* 34, 1 (2018), 1–9.

[56] Elizabeth Hoge, David Bickham, and Joanne Cantor. 2017. Digital media, anxiety, and depression in children. *Pediatrics* 140, Supplement_2 (2017), S76–S80.

[57] Judith A Holton. 2007. The coding process and its challenges. *The Sage handbook of grounded theory* 3 (2007), 265–289.

[58] Michael Horvat, Ron Croce, and James Zagrodnik. 2010. Utilization of sensory information in intellectual disabilities. *Journal of Developmental and Physical Disabilities* 22 (2010), 463–473.

[59] Anastasia Hronis, Lynette Roberts, and Ian I Kneebone. 2017. A review of cognitive impairments in children with intellectual disabilities: Implications for cognitive behaviour therapy. *British Journal of Clinical Psychology* 56, 2 (2017), 189–207.

[60] Li-Ru Hsu and Simone van der Hof. 2023. Fostering inclusivity for children with intellectual disabilities through data protection by design. *European Journal of Law and Technology* 14, 3 (2023).

[61] Elham Hussein, Ashraf Kan'An, Abeer Rasheed, Yousef Alrashed, Malek Jdaitawi, Ahmed Abas, Sherin Mabrouk, and Mona Abdelmoneim. 2023. Exploring the impact of gamification on skill development in special education: A systematic review. *Contemporary Educational Technology* 15, 3 (2023), ep443.

[62] Richard Ingersoll, Elizabeth Merrill, Daniel Stuckey, Gregory Collins, and Brandon Harrison. 2021. The demographic transformation of the teaching force in the United States. *Education Sciences* 11, 5 (2021), 234.

[63] Mizuko Ito. 2013. *Hanging out, messing around, and geeking out: Kids living and learning with new media*. The MIT press.

[64] Jun Izawa, Sarah E Pekny, Mollie K Marko, Courtney C Haswell, Reza Shadmehr, and Stewart H Mostofsky. 2012. Motor learning relies on integrated sensory inputs in ADHD, but over-selectively on proprioception in autism spectrum conditions. *Autism research* 5, 2 (2012), 124–136.

[65] Carrie James, Emily Weinstein, and Kelly Mendoza. 2019. Teaching digital citizens in today's world: Research and insights behind the Common Sense K–12 Digital Citizenship Curriculum. *Common Sense Media* (2019), 2021–08.

[66] Haiyan Jia, Pamela J Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015. Risk-taking as a learning process for shaping teen's online information privacy behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*. 583–599.

[67] Malin Joleby, Carolina Lunde, Sara Landström, and Linda S Jonsson. 2021. Offender strategies for engaging children in online sexual activity. *Child Abuse & Neglect* 120 (2021), 105214.

[68] Hilda K Kabali, Matilde M Irigoyen, Rosemary Nunez-Davis, Jennifer G Budacki, Sweta H Mohanty, Kristin P Leister, and Robert L Bonner Jr. 2015. Exposure and use of mobile media devices by young children. *Pediatrics* 136, 6 (2015), 1044–1050.

[69] Daniel Kardefelt-Winther, Emma Day, Gabrielle Berman, Sabine K Witting, Anjan Bose, et al. 2020. *Encryption, Privacy and Children's Right to Protection from Harm*. UNICEF Office of Research-Innocenti.

[70] James M Kauffman, Daniel P Hallahan, Paige C Pullen, and Jeanmarie Badar. 2018. *Special education: What it is and why we need it*. Routledge.

[71] Rachel Keighley. 2022. Hate hurts: Exploring the impact of online hate on LGBTQ+ young people. *Women & Criminal Justice* 32, 1-2 (2022), 29–48.

[72] Ahmet Osman Kılıç, Eyup Sari, Husniye Yucel, Melahat Melek Oğuz, Emine Polat, Esma Altinel Acoglu, and Saliha Senel. 2019. Exposure to and use of mobile devices in children aged 1–60 months. *European journal of pediatrics* 178 (2019), 221–227.

[73] Anne V Kirby, Lauren M Little, Beth Schultz, and Grace T Baranek. 2015. Observational characterization of sensory interests, repetitions, and seeking behaviors. *The American Journal of Occupational Therapy* 69, 3 (2015), 6903220010p1–6903220010p9.

[74] P Kotroni, Fotini Bonoti, and Sofia Mavropoulou. 2019. Children with autism can express social emotions in their drawings. *International Journal of Developmental Disabilities* 65, 4 (2019), 248–256.

[75] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2017. 'No Telling Passcodes Out Because They're Private' Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–21.

[76] Priya C Kumar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2019. Privacy and security considerations for digital technology use in elementary schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[77] Robin K Kuriakose, Zainab Khan, David RP Almeida, and Puneet S Braich. 2017. Depression and burden among the caregivers of visually impaired patients: a systematic review. *International Ophthalmology* 37 (2017), 767–777.

[78] Melanie Landon-Hays, Maria B Peterson-Ahmad, and Andrea Dawn Frazier. 2020. Learning to teach: How a simulated learning environment can connect theory to practice in general and special education educator preparation programs. *Education Sciences* 10, 7 (2020), 184.

[79] Yangchool Lee and Bogja Jeoung. 2016. The relationship between the behavior problems and motor skills of students with intellectual disability. *Journal of exercise rehabilitation* 12, 6 (2016), 598.

[80] Huanhuan Li and Su Wang. 2013. The role of cognitive distortion in online game addiction among Chinese adolescents. *Children and youth services review* 35, 9 (2013), 1468–1475.

[81] M Lima, K Silva, I Amaral, A Magalhães, and L De Sousa. 2013. Beyond behavioural observations: a deeper view through the sensory reactions of children with profound intellectual and multiple disabilities. *Child: Care, Health and Development* 39, 3 (2013), 422–431.

[82] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2011. Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. (2011).

[83] Sonia Livingstone and Peter K Smith. 2014. Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of child psychology and psychiatry* 55, 6 (2014), 635–654.

[84] Sonia Livingstone and Mariya Stoilova. 2021. The 4Cs: Classifying online risk to children. (2021).

[85] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. 2019. Children's data and privacy online: growing up in a digital age: an evidence review. (2019).

[86] Lotta Löfgren-Mårtenson. 2008. Love in cyberspace: Swedish young people with intellectual disabilities and the Internet. *Scandinavian Journal of Disability Research* 10, 2 (2008), 125–138.

[87] Lotta Löfgren-Mårtenson, Emma Sorbring, and Martin Molin. 2015. "T@ ngled up in blue": Views of parents and professionals on internet use for sexual purposes among young people with intellectual disabilities. *Sexuality and Disability* 33 (2015), 533–544.

[88] Sana Maqsood and Sonia Chiasson. 2021. "They think it's totally fine to talk to somebody on the internet they don't know": Teachers' perceptions and mitigation strategies of tweens' online risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–17.

[89] Sonali Tukaram Marne, Mahdi Nasrullah Al-Ameen, and Matthew K Wright. 2017. Learning System-assigned Passwords: A Preliminary Study on the People with Learning Disabilities.. In *SOUPS*.

[90] Natasha Marrus and Lacey Hall. 2017. Intellectual disability and language disorder. *Child and adolescent psychiatric clinics of North America* 26, 3 (2017), 539.

[91] Florence Martin, Julie Bacak, Drew Polly, Weichao Wang, and Lynn Ahlgrim-Delzell. 2023. Teacher and school concerns and actions on elementary school children digital safety. *TechTrends* 67, 3 (2023), 561–571.

[92] Giovanna Mascheroni and Kjartan Ólafsson. 2016. The mobile Internet: Access, use, opportunities and divides among European children. *New Media & Society* 18, 8 (2016), 1657–1679.

[93] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI conference on human factors in computing systems*. 2189–2201.

[94] G Roy Mayer, Beth Sulzer, and John J Cody. 1968. The use of punishment in modifying student behavior. *The journal of special education* 2, 3 (1968), 323–328.

[95] Janet E McDonagh and Belinda Bateman. 2012. 'Nothing about us without us': considerations for research involving young people. *Archives of Disease in Childhood-Education and Practice* 97, 2 (2012), 55–60.

[96] Nora McDonald, Alison Larsen, Allison Battisti, Galina Madjaroff, Aaron Massey, and Helena Mentis. 2020. Realizing choice: Online safeguards for couples adapting to cognitive challenges. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 99–110.

[97] Mary L McHugh. 2012. Interrater reliability: the kappa statistic. *Biochemia medica* 22, 3 (2012), 276–282.

[98] John William McKenna, Andrea Flower, and Reesha Adamson. 2016. A systematic review of function-based replacement behavior interventions for students with and at risk for emotional and behavioral disorders. *Behavior Modification* 40, 5 (2016), 678–712.

[99] John William McKenna, Andrea Flower, Terry Falcomata, and Reesha M Adamson. 2017. Function-based replacement behavior interventions for students with challenging behavior. *Behavioral Interventions* 32, 4 (2017), 379–398.

[100] Maura R McLaughlin. 2011. Speech and language delay in children. *American family physician* 83, 10 (2011), 1183–1188.

[101] Helena M Mentis, Galina Madjaroff, and Aaron K Massey. 2019. Upside and downside risk in online security for older adults with mild cognitive impairment. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[102] Guy Merchant. 2012. Mobile practices in everyday life: Popular digital technologies and schooling revisited. *British journal of educational technology* 43, 5 (2012), 770–782.

[103] Natasha Mitter, Afia Ali, and Katrina Scior. 2019. Stigma experienced by families of individuals with intellectual disabilities and autism: A systematic review. *Research in developmental disabilities* 89 (2019), 10–21.

[104] Martin Molin, Emma Sorbring, and Lotta Löfgren-Mårtenson. 2015. Teachers' and parents' views on the Internet and social media usage by pupils with intellectual disabilities. *Journal of Intellectual Disabilities* 19, 1 (2015), 22–33.

[105] Savanthi Murthy, Karthik S Bhat, Sauvik Das, and Neha Kumar. 2021. Individually vulnerable, collectively safe: The security and privacy practices of households with older adults. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–24.

[106] Daniela Napoli. 2018. *Accessible and usable security: Exploring visually impaired users' online security and privacy strategies*. Ph. D. Dissertation. Carleton University.

[107] Peter Nikken and Marjon Schols. 2015. How and why parents guide the media use of young children. *Journal of child and family studies* 24 (2015), 3423–3435.

[108] Chaim Noy. 2008. Sampling knowledge: The hermeneutics of snowball sampling in qualitative research. *International Journal of social research methodology* 11, 4 (2008), 327–344.

[109] Jane Oakhill and Kate Cain. 2000. Children's difficulties in text comprehension: Assessing causal issues. *Journal of Deaf Studies and Deaf Education* 5, 1 (2000), 51–59.

[110] Majeda Al Sayyed Obaid. 2013. The impact of using multi-sensory approach for teaching students with learning disabilities. *Journal of International Education Research* 9, 1 (2013), 75.

[111] Susan B Palmer, Michael L Wehmeyer, Daniel K Davies, and Steven E Stock. 2012. Family members' reports of the technology use of family members with intellectual and developmental disabilities. *Journal of Intellectual Disability Research* 56, 4 (2012), 402–414.

[112] Stamatios Papadakis and Michail Kalogiannakis. 2017. Mobile educational applications for children: what educators and parents need to know. *International Journal of Mobile Learning and Organisation* 11, 3 (2017), 256–277.

[113] Jeong Hye Park and Minjung Park. 2021. Smartphone use patterns and problematic smartphone use among preschool children. *PloS one* 16, 3 (2021), e0244276.

[114] Charlie Parker, Sam Scott, and Alistair Geddes. 2019. Snowball sampling. *SAGE research methods foundations* (2019).

[115] Nick Pendar. 2007. Toward spotting the pedophile telling victim from predator in text chats. In *International Conference on Semantic Computing (ICSC 2007)*. IEEE, 235–241.

[116] Maria Peterson-Ahmad. 2018. Enhancing pre-service special educator preparation through combined use of virtual simulation and instructional coaching. *Education Sciences* 8, 1 (2018), 10.

[117] Judith Pinborough-Zimmerman, Robert Satterfield, Judith Miller, Deborah Bilder, Shaheen Hossain, and William McMahon. 2007. Communication disorders: Prevalence and comorbid intellectual disability, autism, and emotional/behavioral disorders. (2007).

[118] Jenny Radesky, Dimitri Christakis, David Hill, Nusheen Ameenuddin, Yolanda Chassiakos, Corinn Cross, Jenny Radesky, Jeffrey Hutchinson, Rhea Boyd, Robert Mendelson, et al. 2016. Media and young minds. *Pediatrics* 138, 5 (2016).

[119] Hakan Sarıçam and Halis Sakız. 2014. Burnout and teacher self-efficacy among teachers working in special education institutions in Turkey. *Educational Studies* 40, 4 (2014), 423–437.

[120] Martin Sas, Maarten Denoo, and Jan Tobias Mühlberg. 2023. Informing Children about Privacy: A Review and Assessment of Age-Appropriate Information Designs in Kids-Oriented F2P Video Games. *Proceedings of the ACM on Human-Computer Interaction* 7, CHI PLAY (2023), 425–463.

[121] Joachim Schüz. 2005. Mobile phone use and exposures in children. *Bioelectromagnetics* 26, S7 (2005), S45–S50.

[122] Leslie Regan Shade and Rianka Singh. 2016. "Honestly, we're not spying on kids": School surveillance of young people's social media. *Social Media+ Society* 2, 4 (2016), 2056305116680005.

[123] Abha Shree and Prakash C Shukla. 2016. Intellectual Disability: Definition, classification, causes and characteristics. *Learning Community-An International Journal of Educational and Social Development* 7, 1 (2016), 9–20.

[124] Kurt Squire and Seann Dikkers. 2012. Amplifications of learning: Use of mobile media devices among youth. *Convergence* 18, 4 (2012), 445–464.

[125] Zahra Stardust, Abdul Obeid, Alan McKee, and Daniel Angus. 2024. Mandatory age verification for pornography access: Why it can't and won't 'save the children'. *Big Data & Society* 11, 2 (2024), 20539517241252129.

[126] Jennifer Stephenson and Lisa Limbrick. 2015. A review of the use of touch-screen mobile devices by people with developmental disabilities. *Journal of autism and developmental disorders* 45 (2015), 3777–3791.

[127] Marc J Tassé, Ruth Luckasson, and Margaret Nygren. 2013. AAIDD proposed recommendations for ICD–11 and the condition previously known as mental retardation. *Intellectual and developmental disabilities* 51, 2 (2013), 127–131.

[128] Carla J Thompson. 2011. Multi-Sensory Intervention Observational Research. *International Journal of Special Education* 26, 1 (2011), 202–214.

[129] Zehra Topal, Nuran Demir Samurcu, Sarper Taskiran, Ali Evren Tufan, and Bengi Semerci. 2018. Social communication disorder: A narrative review on current insights. *Neuropsychiatric disease and treatment* (2018), 2039–2046.

[130] Cary E Trump, Robert C Pennington, Jason C Travers, Joel E Ringdahl, Erinn E Whiteside, and Kevin M Ayres. 2018. Applied behavior analysis in special education: Misconceptions and guidelines for use. *Teaching Exceptional Children* 50, 6 (2018), 381–393.
[131] Barbara A Turner. 2023. *Handbook of sandplay therapy.* Temenos Press.
[132] Eli Vakil, Edna Shelef-Reshef, and Rachel Levy-Shiff. 1997. Procedural and Declarative Memory Processes: Individuals With and Without Mend Retardation. *American Journal on Mental Retardation* 102, 2 (1997), 147–160.
[133] Johann van der Sandt. 2024. Singing in music education as a tool for the development of children's communication skills. *The Literacy, Preliteracy and Education Journal* 8, 3 (2024).
[134] M Van Nieuwenhuijzen and A Vriens. 2012. (Social) Cognitive skills and social information processing in children with mild to borderline intellectual disabilities. *Research in developmental disabilities* 33, 2 (2012), 426–434.
[135] Radu-Daniel Vatavu. 2017. Visual impairments and mobile touchscreen interaction: state-of-the-art, causes of visual impairment, and design guidelines. *International Journal of Human–Computer Interaction* 33, 6 (2017), 486–509.
[136] Ramiah R Vickers and Jane S Gibson. 2019. A review of the genomic analysis of children presenting with developmental delay/intellectual disability and associated dysmorphic features. *Cureus* 11, 1 (2019).
[137] Sandrine Vieillevoye and Nathalie Nader-Grosbois. 2008. Self-regulation during pretend play in children with intellectual disability and in normally developing children. *Research in developmental disabilities* 29, 3 (2008), 256–272.
[138] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper, and Kurt Thomas. 2022. Sok: A framework for unifying at-risk user research. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2344–2360.
[139] Mark Warner, Andreas Gutmann, M Angela Sasse, and Ann Blandford. 2018. Privacy unraveling around explicit HIV status disclosure fields in the online geosocial hookup app Grindr. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 1–22.
[140] Renee Watling and Ilene S Schwartz. 2004. Understanding and implementing positive reinforcement as an intervention strategy for children with disabilities. *AJOT: American Journal of Occupational Therapy* 58, 1 (2004), 113–117.
[141] I Wayan Widana, I Wayan Sumandya, I Wayan Citrawan, I Nengah Suka Widana, Florante P Ibarra, Rosario F Quicho, MRHM Delos Santos, Jennifer V Velasquez-Fajanela, and Amirul Mukminin. 2023. The effect of teacher's responsibility and understanding of the local wisdom concept on teacher's autonomy in developing evaluation of learning based on local wisdom in special needs school. *Journal of Higher Education Theory and Practice* 23, 10 (2023), 152–167.
[142] Krista M Wilkinson and William J McIlvane. 2013. Perceptual factors influence visual search for meaningful symbols in individuals with intellectual disabilities and Down syndrome or autism spectrum disorders. *American Journal on Intellectual and Developmental Disabilities* 118, 5 (2013), 353–364.
[143] Pamela Wisniewski. 2018. The privacy paradox of adolescent online safety: A matter of risk prevention or risk resilience? *IEEE Security & Privacy* 16, 2 (2018), 86–90.
[144] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M Carroll. 2017. Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety?. In *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*. 51–69.
[145] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2017. Parents just don't understand: Why teens don't talk to parents about their online risk experiences. In *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*. 523–540.
[146] Frank H Wood and K Charlie Lakin. 1982. Punishment and aversive stimulation in special education: Legal, theoretical and practical issues in their use with emotionally disturbed children and youth. (1982).
[147] World Health Organization. 2025. ICD-11 for Mortality and Morbidity Statistics. https://icd.who.int/browse/2025-01/mms/en#605267007 Accessed: 2025-03-20.
[148] Raja Zahilah and Siti Zahidah Zaharan. 2022. EyeKids: Real-time tracking and monitoring system for child safety. *International Journal of Innovative Computing* 12, 2 (2022), 1–8.
[149] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. I make up a silly name' Understanding Children's Perception of Privacy Risks Online. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–13.
[150] Lin Zhu, Yan Wang, and Yanhong Chen. 2025. Sharenting in China: perspectives from mothers and adolescents. *Internet Research* 35, 1 (2025), 105–125.

# A EXCLUSION METHOD

Before conducting the interviews, we guided potential participants to answer the following questions to determine their involvement in managing their child's digital safety.

For parents, we primarily asked:

- Has your child been diagnosed with intellectual disability?
- How old is your child? What grade are they in?
- What types of mobile devices does your child use daily (e.g., smartphone, tablet, smartwatch)?
- What is the frequency of your child's mobile device usage?
- What activities does your child primarily use these mobile devices for (e.g., entertainment, communication, etc.)?

For teachers, we primarily asked:

- Are you a teacher at a special education school or a rehabilitation institution?
- How many years of experience do you have in this field?
- Does your institution allow students to use personal devices?
- What types of mobile devices do you observe your students using regularly (e.g., smartphone, tablet, smartwatch)?
- What activities do you observe your students primarily using these mobile devices for (e.g., entertainment, communication, learning, etc.)?

These questions helped us exclude parents and teachers who belong to special education but are not involved in the digital safety practices of children.

# B INTERVIEW PROTOCOL

***Opening***. Thank you for participating in our research. My name is ***, and I am a researcher at ***. Our study aims to understand how you perceive and address the digital safety challenges faced by children with intellectual disabilities. Throughout the interview, I will ask you a series of questions. There are no right or wrong answers; please respond based on your actual experiences. If you find any question uncomfortable, you may skip it. You can also ask questions or pause the interview at any time, and this will not affect your participation compensation.

We value your unique experiences and opinions. The interview will be recorded for research purposes, but the recording will not be made public, and your identity will remain confidential. Do you agree to the recording and to start the interview?

## B.1 Interview Protocol with Parents

- What is your age?
- What is your occupation?
- What is your child's age, grade, gender, and where do they receive their education?
- What type of diagnosis does your child have?
- Does your child exhibit any stereotypical behaviors, social impairments, or self-stimulatory behaviors?
- How is your child's ability to express themselves?
- How are your child's learning and comprehension abilities? Do they require special techniques or methods when being taught new knowledge or skills?
- Does your child have their own mobile device?
- What mobile device does your child use most frequently, and what is its primary purpose?
- Was the device specifically purchased for your child, or is it a parent's device that is given to the child with restrictions?

- What factors do you prioritize when selecting a device?
- Do you establish any rules in advance? What considerations are these rules based on?
- What do you typically do when giving the device to your child? Do you set any configurations or teach them how to use it?
- What applications are installed on your child's mobile device? Do you manage or configure these applications in any way?
- Do you conduct regular checks on the device after giving it to your child? What do you focus on during these checks?
- What do you check for? Are there any features you have thought of reconfiguring or disabling during use?
- Do you believe your child has the ability to use a mobile device independently?
- Do you supervise your child while they use the mobile device?
- What obstacles do you think your child might encounter when independently operating a mobile device? What impacts might these obstacles have?
- Do you have any concerns about your child's use of the device?
- Have there any specific actions your child takes that lead to your concern?
- Have you ever been concerned about any information your child has encountered on the device?
- What specific actions or information cause you concern? Has anything specific happened to prompt these concerns?
- How do you address these concerns?
- How do you teach your child to distinguish the correctness of content? How do you teach them what is safe and how to recognize safety risks in mobile devices?
- Do you limit daily usage time? What is the purpose of this limitation, and is it effective?
- Do you restrict app downloads? Which types of apps do you restrict, and what is the purpose of this restriction? Is it effective?
- Do you enable kids mode? Do you focus on this mode, and what is the purpose of enabling it? Is it effective?
- Are there any special restrictions on internet usage?
- Do you feel comfortable with your child taking the mobile device to school?
- Are you concerned about any safety risks associated with your child bringing the mobile device to school?
- Have you specifically instructed teachers to supervise your child's use of the mobile device?

## B.2 Interview Protocol with Teachers

- What is your age?
- How long have you been working at the special education school?
- What type of children do you primarily work with? What are the specific characteristics of these children?
- What subjects and grade levels are you primarily responsible for teaching?
- Does the school provide opportunities for children to access digital resources?
- Do children have any tasks at school that require the use of mobile devices?
- Have you observed whether children have their own mobile devices? What is the ratio of ownership and usage of mobile devices?
- Do children carry mobile devices with them daily?
- What do children use mobile devices for on a daily basis?
- What settings and checks do teachers perform on students' mobile devices?
- Do you remind children to pay special attention when using mobile devices?
- Do you establish any rules in advance? What considerations are these rules based on?
- What communication techniques do you use with children? What communication methods are most acceptable to them?
- How do you teach children to distinguish the correctness of content? How do you teach them to differentiate between good and bad people? How do you teach them what is safe?
- Does the school organize courses to teach children how to use mobile devices?
- Have you personally organized teaching activities to instruct children on how to use mobile devices?
- Do you communicate with parents about their children's use of mobile devices?
- What specific content do you discuss? Is it about the constraints on the children?
- How do teachers assist or supervise children in using mobile devices? Are there any measures or management methods?
- Have children encountered any problems while using mobile devices daily?
- What risks do you think children face when independently operating mobile devices? In what usage scenarios? When using them for what purposes?
- What specific operations or information cause you concern?
- Are you worried about any specific actions children might take that could lead to problems?
- Are you concerned about the information children might encounter on mobile devices? Why?
- Do you think the degree of impact on children is intensified because they have intellectual disabilities, or is it because they are children?
- How do you think children's use of mobile devices should be restricted and regulated? For example, should daily usage time be limited? Should app downloads be restricted? Should kids mode be enabled? Are these measures effective?

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009