TechTrends (2023) 67:561–571
https://doi.org/10.1007/s11528-022-00803-z

ORIGINAL PAPER

Teacher and School Concerns and Actions on Elementary School Children Digital Safety

Florence Martin[1] · Julie Bacak[2] · Drew Polly[2] · Weichao Wang[2] · Lynn Ahlgrim-Delzell[2]

Accepted: 1 October 2022 / Published online: 7 October 2022

Abstract

Elementary school children are spending more time using digital technologies. Teachers and schools are concerned about the student's digital safety. We interviewed ten elementary school teachers virtually to understand their concerns and understand the actions they take regarding elementary school children's digital safety. Using thematic analysis, we identified themes of concerns and actions of teachers and schools on elementary school children's digital safety. Some digital safety concerns discussed by the teachers included content-related concerns such as accessing inappropriate content, contact-related concerns, inappropriate contact with others online, sharing personal information, lack of understanding of danger, conduct-related concerns regarding cyberbullying and digital footprint, contract-related concerns such as digital security and privacy, and home-related concerns. Teachers and schools have taken several actions to address these concerns. Some of the digital safety actions included security measures and limits, monitoring student activities, providing education on digital safety, and support from guidance counselors. This study has implications for elementary school educators, administrators, parents, and students on the safe use of digital technologies.

Keywords Digital safety · Elementary school children · Digital safety concerns · Digital safety actions

Digital exposure and usage, both in and outside of school, by students as young as elementary school-age have become evident in our current digital society (Stoilova et al., 2019; Martin et al., 2021). In addition to using technology for learning purposes, children have access to mobile devices and participate in online video games and use social media even while in elementary school (Rideout & Robb, 2019). Therefore, fostering and facilitating the dynamics of healthy behaviors in using digital devices is essential to producing responsible twenty-first-century learners in our schools and communities (UN, 2021).

Digital Safety Concerns

Digital technologies give children today more access to information and more freedom to interact with others online. While increased access presents many opportunities for learning and social connections, it also poses potential risks. Aftab (2000) categorizes six types of risks that children face online: exposure to inappropriate information, exposure to potentially dangerous information, being stalked or harassed, disclosure of important and private information, online-purchase scams, and enticement by cyber-predators who want to meet children face-to-face. Aftab (2000) indicates that children have some level of control over most of these risks, highlighting the importance of digital safety education beginning at an early age. In this study, we specifically focus on digital safety concerns such as cyberbullying, digital security, digital privacy, digital footprint, and digital identity. Table 1 describes the different digital safety elements.

✉ Florence Martin
Fmartin3@ncsu.edu

Julie Bacak
jabacak@uncc.edu

Drew Polly
abpolly@uncc.edu

Weichao Wang
WeichaoWang@uncc.edu

Lynn Ahlgrim-Delzell
laahlgri@uncc.edu

[1] North Carolina State University, Raleigh, NC, USA

[2] University of North Carolina Charlotte, Charlotte, NC, USA

Table 1 Digital Safety Elements

Digital Safety Elements	Description
Cyberbullying	Cyberbullying is harassment that takes place over digital devices like cell phones, computers, and tablets.
Digital Footprint	A digital footprint is a trail of data one creates while using the Internet.
Digital Privacy	Digital Privacy refers to the confidentiality of the digital information shared.
Digital Netiquette	Digital netiquette is formal or informal rules that apply when communicating online.
Digital Identity	Digital Identity refers to how one perceives oneself and how others perceive the person based on the person's online activity.

Social Connections through Social Media and Video Games

The ease of access to digital technology also contributes to children accessing social media at a young age. While traditional media is designed to be used by those 13 years and older, Rideout and Robb (2019) found that among 16- to 18-year-olds included in a national survey study, 28% of teen social media users reported using social media for the first time before age 13. Research on the impact of youth social media use shows some positive outcomes related to maintaining social connections with peers, yet youth social media use is also linked to increased depression, reduced self-image, and increased cyberbullying (Richards et al., 2015). When examining the link between parental control over time spent on social media and the mental health of 10–12 year old girls, Fardouly et al. (2018) identified better mental health outcomes for girls whose parents had more control over the time they spent on social media. There are few studies that relate specifically to the effects of social media use on elementary-aged students with most of the research aimed at teens and young adults.

In addition to traditional forms of social media, young children are also interacting with others when playing online video games. Among children 8 to 12 years old included in a national survey study in the United States, 53% of screen time is devoted to watching TV or online videos, and 31% of screen time is spent playing video games (Rideout & Robb, 2019). The prevalence of frequent online video game play is concerning as online games are a common site for cyberbullying in children 8 to 12 years old. DePaolis and Williford (2015) conducted a survey study of nearly 700 third through fifth grade students. They found that almost 18% of participants had experienced some form of cybervictimization, mostly through online games; over half of these children did not know the identity of the perpetrator of the action.

Digital Security and Privacy

While children know how to access the online world at a young age, they do not yet know how to navigate this world safely in terms of privacy and security. Through systematic evidence mapping of existing literature, Stoilova et al. (2019) found that children ages 8 to 11 years old are starting to understand the risks of sharing certain information online, but they tend to think about privacy more in terms of interpersonal relationships in which they actively share data rather than aspects of privacy related to commercial data sharing that can have a lasting impact. Similarly, in a qualitative study of families in the United States with children between the ages of 5 and 11 years old, Kumar et al. (2017) found that children under ten years old demonstrated little understanding of how sharing information online can lead to privacy concerns; older children in this study demonstrated developing understanding. Children in this age group rely heavily on the adults in their lives to ensure their privacy and safety (Stoilova et al., 2019), but parents largely use passive strategies to mediate their child's device and view online privacy lessons as something to address in the future when their child is older (Kumar et al., 2017).

Teacher Concerns

Most of the research related to digital safety concerns for children offers the perspectives of researchers or parents. Few studies directly identify teachers' concerns about their young students' digital safety. Martin and colleagues (2019) conducted a survey study of K-12 educators' perceptions of their students' digital citizenship practices. In this study, teachers across grade levels reported that practices related to digital footprint and digital identity were not well understood or followed by their students. In a nationally representative survey study of K-12 teachers, Vega and Robb (2019)

summarized teachers' top technology-related concerns based on their observations of student interactions. While the top concerns identified in this study were not directly related to digital safety, 25% of teachers in grades 3–5 (ages 8 to 11) reported at least occasional cyberbullying among their students, indicating a need to address these safety concerns at a young age.

Teacher and School Actions

Parents are often the first guides for young children interacting in the online world, but as students increasingly use digital technologies for learning and communication at school, teachers also play an important role in keeping children safe online. Teachers support the digital safety of their students by developing their own professional knowledge of digital safety, modeling best practices for students, and teaching students about how to stay safe online.

Teachers Professional Development on Digital Safety

To encourage digital safety among students, teachers and administrators must have current knowledge and awareness of digital safety topics (Hollandsworth et al., 2017). Teachers can support the digital safety of their students by participating in digital safety professional development (PD). Martin and colleagues (2022) offered PD for teachers on digital citizenship covering topics such as cyberbullying, digital footprints, digital identity, digital privacy, and digital netiquette. Participants reported the benefits of participating in this PD, especially from the opportunity to develop digital safety lessons to use with students.

Berger and Wolling (2019) conducted a survey study of over 300 teachers in Germany to better understand factors associated with teachers' practices to support students' digital safety skills. Findings revealed that teachers with greater knowledge of digital safety guidelines were more likely to attribute high importance to digital safety skills and were more likely to integrate these topics into their classroom instruction.

Teachers' Incorporating Digital Safety Lessons

Another action teachers can take to help keep young learners safe online is to incorporate digital safety and digital citizenship lessons into instruction. As with other types of safety instruction, Jones and Mitchell (2016) support a proactive approach to teaching digital safety on an ongoing basis rather than promoting fear-based strategies in response to students' demonstrating unsafe behaviors. A recent survey of educators in the United States shows that digital citizenship competencies are most heavily incorporated into instruction at the secondary level, not the elementary grades when a proactive approach would be more relevant (Vega & Robb, 2019). Specifically looking at elementary school teachers, Kumar et al. (2019) found few instances of elementary students receiving lessons on digital privacy and security within their focus group research. When lessons were taught related to privacy and security, they typically came from the school media specialist.

Late elementary school presents an ideal time to teach students about how to curate their digital footprint. In Australia, Buchanan et al. (2017) conducted focus groups with 10–12 year old students and found that children in this age group were aware of their digital footprint, but they did not understand the potential positive impact of a well-curated digital footprint. The dominant narrative around digital footprint is presented to students as a liability to be minimized, but Buchanan et al. (2017) advocate for teaching elementary students explicit skills to develop a positive digital footprint for their future.

Monitoring Student Online Behaviors

Another action that teachers and administrators take in addition to educating their students on the importance of digital safety is monitoring the student online behaviors. Growing concerns about students' digital safety have led to schools and districts implementing technology to surveil students' online activity through third-party applications and software (Burke & Bloss, 2020; Shade & Singh, 2016). Monitoring student activity attempts to reduce or prevent bullying and threats of violence targeting individuals or schools (Shade & Singh, 2016), though there is insufficient evidence to support the effectiveness of this type of monitoring in protecting students as intended (Burke & Bloss, 2020). Some school districts also invest in software to monitor students' digital use on school devices. They track students' browsing history, and monitor words in email exchanges and other activities on the learning management systems to monitor any inappropriate behaviors (Lester, 2018).

School-Wide Initiatives and Partnerships

One way to promote students' digital safety is through school wide initiatives. With regard to cyberbullying awareness and prevention, Couvillon and Ilieva (2011) recommend ongoing school wide initiatives as the most effective and practical as schools have the ability to connect with all groups involved, including parents and community members. School and family collaboration supports consistent, up-to-date messaging about how to support childrens' digital safety (Mark & Nguyen, 2017). Buchanan (2021) likewise advocates for school and community partnerships to help children develop strategies for curating digital footprints.

While building partnerships with parents and communities is largely seen as an asset in supporting children's digital safety, differing views and unclear boundaries for responsibility between home and school can present barriers to digital safety efforts. Young et al. (2017) found that while school administrators identified cyberbullying as a major problem, they were uncertain about appropriate actions and prevention measures to take at school. This uncertainty is due in part to lack of consistent messaging about cyberbullying at home versus school.

Purpose of the Study and Research Questions

In a prior study, Martin et al.'s (2021) examined the perceptions of parents of elementary school students about their children's digital safety and found that parents were concerned all the time about their child's digital safety with the biggest concern being their kids being exposed to sexual content and them talking to strangers. Apart from home, students spend the most amount of time at their school. Building on the Martin et al. prior study (2022), we interviewed ten elementary school teachers to get their perspective on what concerns they have regarding elementary school children's digital safety and what actions they and their schools take to keep the children safe. The research questions include:

1. What are teachers' biggest concerns about students' digital safety?
2. What are teachers and schools doing to keep the children safe?

Methods

In order to examine the research questions, the authors interviewed ten elementary school teachers about their perceptions of elementary school children's digital safety using a qualitative research method. Institutional Review Board approval was received from the researchers' institution before the study commenced. More details about the methodology of the study are included in the sections below.

Conceptual Framework

Researchers reiterate the importance of considering the benefits the online environment affords, not just the risks (Livingstone & Stoilova, 2021). The International Society for Technology in Education (ISTE) in Standard 2 for students focuses on the student being a digital citizen (ISTE, 2019). The Standard states that students should "recognize the rights, responsibilities, and opportunities of living, learning and working in an interconnected digital world, and...act and model in ways that are safe, legal and ethical" (p. 1). The substandard for students focuses on aspects of digital netiquette, digital identity, digital security, digital privacy, and cyberbullying, and demonstrates the importance of digital citizenship in today's education (Table 1). This was used to develop the interview questionnaire.

In addition, we use Livingstone and Stoilova's (2021) updated 4Cs framework to guide the data analysis for the concerns (Fig. 1). The 4Cs included content risk, contact risk, conduct risk, and contract risk and were created as part of the "classifying online risk to children" project funded by the European Union aimed to support children and youth through research, policy and practice. Content risk exists when children are exposed to inappropriate or potentially harmful information or images online. Contact risk is present when children are engaged in potentially harmful communication with others, such as in instances of grooming or solicitation. Conduct risk includes children witnessing, participating in, or falling victim to harmful or inappropriate behaviors online, such as cyberbullying. Contract risk involves exploitation of children for commercial interest, which includes risks to digital privacy and security.

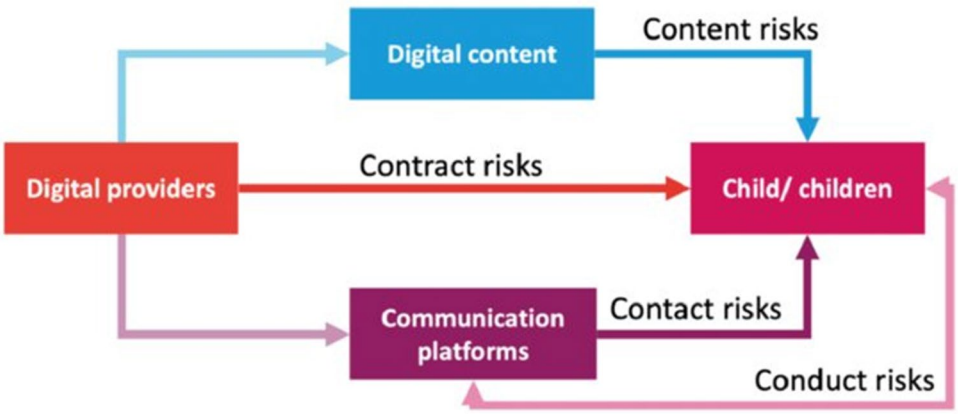

Fig. 1 Four Cs′ by Livingstone and Stoilova (2021). Author permission received

Research Design

This study used a qualitative approach to gain insight into the research questions by exploring teacher's experiences on student digital safety. The goal of basic qualitative research is to "understand how people make sense of their lives and their experiences" (Merriam & Tisdell, 2014, p. 24). This study sought to understand teachers' concerns and actions with digital safety in their elementary classrooms and a basic qualitative approach was suitable (Kahlke, 2014; Percy et al., 2015).

Instrument

The research team developed a semi-structured interview protocol with 11 questions aligned with the ISTE Standard 2 focused on digital citizenship to guide the interview process and collect in-depth qualitative information. The researchers met twice to review the questions for clarity and intent. All the questions were open-ended with the opportunity to ask follow-up questions as needed. The interview questionnaire is included in the Appendix A.

Participants

Classroom teachers and teachers who work as technology facilitators in elementary schools, teaching Kindergarten through Grade 5 (ages 5 through 11) in a southeastern state in the United States were invited to participate in this study. Technology facilitators are teachers who work across grade levels in their school site to support instruction with technology. Requests for interviews were also shared through social media groups that teachers were part of. The definitions of the various digital safety terms used in the interview questions were shared with the teachers at the start of the interview. Ten teachers agreed to participate in the 30-minute interviews. All teachers were female and they taught different elementary grades. While seven teachers had received professional development on digital safety, three teachers had not. The ten teachers all worked at different schools across four public school districts, a public charter school, and a local private school. Table 2 includes the demographic characteristics of the teachers who were interviewed.

Data Collection and Data Analysis

The second author conducted most of the interviews synchronously online via Zoom while the first author joined a few of the interviews. The interviews ranged from 20 to 30 minutes. While consent to participate in the interview was requested early on, this was reinforced before the recording began. The interviews were transcribed by machine-based Otter transcription, and then further cleaned manually.

The interview responses were compiled by questions and then two inductive coding cycles were used by two researchers who read each interview. Initial codes were derived from open coding of the first three transcripts. The team members met to discuss initial coding and created a codebook of agreed upon codes from these first three interviews. The first three interviews were recoded based on the shared codebook before coding the remaining transcripts. Additional codes were added, as needed. Interrater reliability was 90.1% based on the initial coding. Disagreement were discussed until agreement was made with the two coders. Once all interviews were coded, the two researchers organized codes into axial codes (Strauss & Corbin, 1990) based on the common patterns of response. Similar codes were further categorized using thematic analysis techniques (Saldaña, 2021).

Trustworthiness is demonstrated in this study in multiple ways. First, the interviews were coded by two independent coders, then compared for agreement. Disagreements were discussed until a consensus was reached. Second, teachers

Table 2 Teacher Participant Demographic Characteristics

Teacher	Gender	Years of Exp.	Grades Taught	Prior Professional Development on Digital Safety	Teacher or Technology Facilitator
A	female	14	2, 3, 4	Yes	Teacher
B	female	15+	mostly k-5, some middle and high school	Yes	Teacher
C	female	6	2, 3	No	Teacher
D	female	8	k-5	No	Teacher
E	female	2	4	Yes	Teacher
F	female	1	3	Yes	Teacher
G	female	17	4, k-6	Yes	Technology Facilitator
H	female	14	3, 4, 5, k-5	Yes	Technology Facilitator
I	female	9	3	no	Teacher
J	female	7	2, 3–5	yes	Technology Facilitator

were sent a copy of their transcript to examine for accuracy and an opportunity to provide additional comments through member checking. No changes were made as a result of the teacher reviews. Third, the initial codes were discussed with the entire team including experienced researchers on digital safety and coding to identify additional themes.

Positionality Statement

The second author took the lead on conducting interviews and analyzing data for this study. She is a former classroom teacher and current doctoral student. At the time of the study, she had recently moved to the area where this study was conducted and had no prior connections to the participants or the school districts where they worked. The lead author participated in a few interviews, but she had no prior connections to the participants as well. While other authors supported data analysis through initial independent coding and confirmation of codes, all data was shared with other members of the team with participant identifiers removed to minimize potential bias towards participants or schools where they have established relationships.

Results

In this section we present the findings from the interviews in the following sections: 1) teachers' concerns and 2) teachers' and school actions on students' digital safety. Teacher concerns are discussed through content-related concerns such as accessing inappropriate content, contact-related concerns, inappropriate contact with others online, sharing personal information, lack of understanding of danger, conduct-related concerns regarding cyberbullying and digital footprint, contract-related concerns such as digital security and privacy, and home-related concerns. Teachers and schools' actions included security measures and limits, monitoring student activities, providing education on digital safety and support from guidance counselors.

Teachers Concerns about Students' Digital Safety

Teachers discussed several overall digital safety concerns. The concerns were categorized based on the 4Cs (content, contact, conduct, and contract) framework proposed by Livingstone and Stoilova (2021). An additional theme specific to home-related concerns was also mentioned by the teachers.

Content-Related Concerns Content-related concerns included examples of students accessing inappropriate content. Some of the inappropriate content teachers mentioned included students attempting to access inappropriate images, pornography, and gambling websites. Teacher J specifically mentioned a student searching the word, *"naked," but "spelled n-a-c-k-e-d."* The same teacher shared an incident in which she was able to intervene when a child was attempting to access a pornagraphic website. When asked if she thought the child was deliberately attempting to access this content or simply stumbled upon it accidentally, she confirmed that these attempts were intentional. In these instances, teacher participants conveyed that it is important to note that technologies and supervision school districts had in place, such as content filters, prevented children accessing the inappropriate content.

Contact-Related Concerns Contact-related concerns included inappropriate contact with strangers online, friending other people and sharing personal information, without understanding the potential risk. Teacher B commented, "I don't think they understand. I think they think it's a game. And those people aren't real. And there's no real threat there." When describing the types of information students are sharing online, Teacher C commented, "[they are] sharing maybe their first name or information about themselves while playing video games or on social media. They don't know yet what's harmful to them. So, they don't know how they should stay away from it." Teacher J described students' interactions with others online as naive. "They don't know who they're interacting with. They think it's another second grader, but it's not necessarily." Overall participants' responses expressed the importance of educating elementary school students on some of these digital safety topics about understanding the risk of sharing personal information and the difference between appropriate and inappropriate contact with others online.

Conduct-Related Concerns Participants described conduct-related concerns about cyberbullying and students' awareness of their digital footprint. Teachers described negative uses of technology through inappropriate peer interactions. Teachers shared that elementary school children have experienced cyberbullying even though they sometimes have trouble identifying what it really is. Teacher F commented, "Some boys would message one of my girls and just call her dumb and annoying and rude. They would private message it on Google Classroom." Based on the participants' perspectives, elementary school children do not know how to collect evidence of cyberbullying. Teachers also stated that there is online bullying that has occurred on social media platforms. When students were synchronously online during Covid-19, Teacher H mentioned "within our Microsoft Teams, students have found ways to get into chats that we didn't know you could. And they'll pick on each other." Teacher I shared, "My AIG (Academically and Intellectually Gifted) students figured out that they could cuss at each other by putting the

letters in all white and then highlighting it with white. So you didn't see it in the background unless you highlighted it with your mouse."

Participants expressed that students also struggle with understanding the concept of digital footprint, that something they post today can be found by a future employer when they are 25. Teacher B shared a conversation she had with a student about a video he posted and later deleted:

> He says, 'it's fine, because I deleted it.' And I said, 'it's not, it's always going to be there.' Also, fourth and fifth graders, they don't care what they put out there. And then when you bring it back up on the screen 15 minutes later, they thought it was gone. They absolutely panic.

Participants' responses demonstrated the need for education and awareness on the digital safety of cyberbullying and digital footprint topics.

Contract-Related Concerns Participants reported contract-related concerns focused on issues of digital security and privacy. According to the teachers in this study, their elementary school children do not understand that they should not be sharing passwords. Additionally, teachers discussed that elementary school students are not aware of the importance of digital security and privacy. Because of this, some teachers shared how they assist students by educating them about security, such as protecting passwords and limiting access to certain apps or websites. Teacher B commented, "They are learning the difference between personal, private, and public information."

Home-Related Concerns Teachers mentioned several home-related concerns regarding digital safety, emphasizing the need for parents to be actively involved in their child's safety online. Teacher I commented "some of the things that they get to do at home kind of transpose over into school. They've learned some bad routines…not really bad, but things that older kids are able to do. And it's getting younger and younger." In addition, Teacher J mentioned, "the lack of parental supervision with technology really astounds me. And the fact that we're just giving them phones and stuff like that, and not really teaching them like, 'hey, this could get you in serious trouble.'" They recommended that it is important for parents to monitor who their children are talking to online rather than letting them do whatever they want. They also mentioned that "parents need to be aware that their kids are doing this and that they need to play a part in watching them and saying, 'no. You can't go on that right now.'" Participants' responses demonstrated the need for parental supervision at home so that the things they do at home do not transpose into the school context. Some teachers also suggested a need for parent instruction on digital safety. They felt that instruction for parents in digital safety would help support consistent messaging between home and school about how to stay safe online.

Teachers and School Actions to Keep the Children Safe Online

Teachers were asked what they and their school do to keep the children safe online. Some of the actions that teachers and schools are taking include security measures and limits, monitoring student activities, providing education on digital safety, and support from guidance counselors.

Including Security Measures and Limits School/school system actions mostly include security measures such as passwords, firewalls, and filters. One teacher commented that her school district has set limits to what can be installed or viewed. If teachers would like to share videos from sites such as YouTube that have to be approved by our district on YouTube. Setting limits on technology tools is a critical action that teachers and schools took to keep the children safe. Teacher H described the systems her school has in place to support students' security:

> We have limited things so much for students. We have a lot of really good filters in place. For example, when they're logged into their school account, they can only watch videos that are approved by administration or people higher up the chain of command. And when our school devices are sent home, they are highly locked down.

Schools also have safe search on Google turned on so that students do not search for inappropriate content.

Monitoring Teachers responded that they monitor the chat on Zoom, and they monitor students' screens. Teachers are able to login to any device and see where the kids are online. One of the commonly used monitoring programs mentioned by the teachers was DYKnow, which schools use to see how the kids are interacting with each other and monitor their computer screens to make sure that they are not distracted. Teacher F shared, "I can set a block, lock their screen and send a private message to just them. It'll pop up on their screen, and they can't click out of it until I unlock it." They also shared that they can also log into any device and see where any kid has been, including keystroke logging. Teacher H mentioned "So if we know we're having trouble with certain specific students, we can turn those options on and really monitor what they're doing and where they are".

Teacher I expressed that the technology department staff receives notifications or alerts when somebody at the school tries to access a restricted website or other restricted content.

Alerts are sent to their email and to their phone. The staff is then able to check into the incident and see if it was a simple typo or if it was somebody repeatedly trying to access that restricted content.

Student Education on Digital Safety Education is another action that teachers and schools took to protect the elementary school children in the digital world. When asked about resources to support digital safety, teachers identified a wide variety of potential instructional content and resources. The most frequently suggested content included information on safety (i.e., protecting their privacy, interacting with strangers), appropriate online behavior, and creating instruction based on the child's age. While a few teachers specifically identified a technology resource, most teachers commented on ways to make the resources accessible to students of all ages (such as kid friendly, developmentally appropriate) and engaging (i.e., fun, gaming, avatars).

Teachers also provided numerous instructional techniques such as tutorials, scenarios, and knowledge checks. Some teachers mentioned how frequent digital safety should be taught and responses ranged from once a year to monthly to weekly. Some teachers also suggested a need for parent instruction on digital safety. Many teachers described how their school/school system provided digital safety instruction such as lessons on general digital safety and cyberbullying and technology resources (i.e., Brainpop, Internet Awesome). Some teachers described creating their own lessons. Some schools do school wide training programs on anti-bullying which includes cyberbullying and about pledging not to bully each other.

Teacher comments include providing students with the knowledge they need so they can act responsibly. Teacher G commented "The biggest thing we try to stress to our students is teaching them to be cautious about who that other person is on the other side of the screen." Teachers also take the time to reinforce the things that elementary school children need to keep in mind when going online, and who to reach out to for assistance. Teachers take the time to educate children on various digital safety topics. Teacher J described some of the advice she shares with her elementary students:

> "I go over with my kids, like you don't share your password with anybody. You don't tell people how old you are. And if it is a site that asks your age, you go get an adult. You don't put in your parents' email for things. You don't make up an email and then put it in there."

Teachers also teach the kids not to leave their laptop logged in on the table, such as when they go to the bathroom. They teach them to log out since you never know who can come in and type some stuff on their device that they are responsible for.

Support from Guidance Counselors Teachers commented that guidance counselors play an important role in digital safety. Students are taught to report any issues to guidance counselors. When specifically addressing how students report cyberbullying, Teacher G shared, "we've taught them to report this to an adult. Or we have bullying forms that they can complete online and submit to our guidance counselor, and they'll help intervene in that way." Guidance counselors also support digital safety education in schools. Teacher H commented "[our guidance counselor] does a lot of education on how to identify what's happening, how to identify your emotions, and how to talk to adults when you're in that situation. Especially if it's something that's happening online."

Discussion

The findings advance the current knowledge about digital safety with elementary school children by sharing teachers' and technology facilitators' perceptions and concerns of childrens' interactions with digital technologies. Building on the framework proposed by Livingstone and Stoilova (2021), the findings were organized around their five areas of teacher concerns and actions. In this section, the authors discuss these in the context of the current literature. First, we discuss teachers' concerns (question 1) and then teachers' actions (question 2).

Teachers' Concerns about Digital Safety

Related to question 1, since the literature does not include a lot of studies focused on elementary school children's digital safety, this study advances the field by sharing teachers' concerns related to digital safety. Findings related to contact-related concerns focused on inappropriate contact with others online, sharing personal information, and lack of understanding of danger. Teachers reported the need to educate students about the potential harms and dangers of contact-related situations.

Additionally, teachers expressed concerns related to content. This finding included concerns about student access to inappropriate content and showed the importance of including security measures such as firewalls, and filters (Hills, 2018). Teachers echoed the findings of Hills's (2018) study by reporting specific experiences where students intentionally tried to access inappropriate content. Teachers also reported and discussed that content-related concerns included the use of digital technologies during the school day as well as outside of school including at children's' homes. Some of the concerns expressed by the teachers about elementary school children accessing inappropriate

content were also expressed by the parents in previous research (Martin et al., 2021).

There were also conduct-related concerns reported by teachers which included cyberbullying and children's digital footprints. These concerns confirm the work of Richards et al. (2015) who found that cyberbullying and inappropriate conduct online were elevated by children's increased access to digital technologies, including apps and social media. Related to contract-related concerns, teachers reported that they were worried about children keeping their digital accounts secure and private, including passwords.

An additional theme specific to home-related concerns included the need for parents to be actively involved in their child's safety online. Some parents do not monitor their children's digital accounts and this behavior transfers into their school. Educating the parents and collaborating with the teachers on monitoring their child's online behavior (Kumar et al., 2017) is very important to avoid home-related concerns.

Teachers' Actions Related to Digital Safety

Question 2 examined the actions of teacher-participants in response to their concerns about their students' digital safety. While the framework provided an overview for Question 1, data analysis indicated that teachers' actions and recommendations heavily overlapped with the various areas of concern. One common theme was the need for filters and processes to block or limit the likelihood of students accessing inappropriate content and/or interacting with strangers while using digital technologies in school. Most schools and school districts are now required by law to have these, and as reported by teachers, schools and school districts have started to establish processes including filters and alerts that notify technology staff when an individual tries to access inappropriate content.

In terms of education, a frequently found theme was the need for schools to take responsibility and be more deliberate about educating children about the dangers and potential harms of online behavior. This includes educating children on online netiquette and also teaching them to collect evidence when they are cyberbullied (DePaolis & Williford, 2015). Educating students on digital footprint (Buchanan et al., 2017) and what they say online can impact their future is important for students to maintain appropriate conduct (Jones & Mitchell, 2016). Also, having them reach out to guidance counselors or teachers when they have been cyberbullied or witness inappropriate online behavior will be helpful. Educating the students on digital security and privacy and helping them differentiate what is public and private information is important. Schools can also put blockers in place where students cannot login with each other's account information. As stated previously, it is important to consider how to effectively educate elementary school-aged children about contact-related dangers. As access to technology with younger children becomes more prevalent these educational experiences and activities are more important than ever.

To summarize, Table 3 includes the concerns based on the 4C's framework, the themes found in this study and the teacher and school actions recommended from this study.

Limitations and Future Directions for Research

While this study contributes to the field by sharing teachers' perceptions and concerns of digital safety for elementary school-aged children, there are some limitations that should be noted. While we employed some of the qualitative techniques, such as member checking, peer debriefing, and involved experienced researchers in coding, one of the limitations is that there was no triangulation of data since the interviews were the only data source. Additionally, there

Table 3 Digital Safety Concerns and Actions for Elementary School Children

	Digital Safety Teacher Concerns	Teacher and School Actions
Content-related	Searching for inappropriate content and accessing inappropriate websites	Educating elementary school students Use of content filters and firewalls Monitoring applications
Contact-related	Inappropriate contact with strangers online Friending other people and sharing personal information without understanding the potential risk	Educating elementary school students on risks Monitoring applications Support from guidance counselors
Conduct-related	Cyberbullying Inappropriate peer interactions Lack of awareness of digital footprint	Education and awareness on cyberbullying and digital footprint Monitoring applications Support from guidance counselors
Contract- related	Lack of awareness of digital security and privacy	Educating about security and privacy such as protecting passwords Limiting access to certain apps or websites
Home-related	Lack of parental monitoring of online activity	Parent education on digital safety

was no prolonged engagement with the interviewee. Though the participants were from different schools, they were all from one state in the United States, so findings may not be generalizable to all settings.

Future research studies on the topic of digital safety with elementary school-aged children should include teachers and technology facilitators from various parts of the country and world, including those from urban, suburban, and rural populations, as well as populations that may differ in socio-economic status. While there is no empirical support, we hypothesize these different populations may yield different findings related to concerns and actions related to digital safety with young children. This work could also be extended to include teacher-participants from middle and high school settings as well. Also, since this data only focused on teacher perception of students' digital safety, it does not take the home school engagement and parent-child-school relationships. These perspectives are also important to be taken into consideration while studying elementary school learners.

In terms of future studies, examinations of elementary school-aged children's digital safety should continue to include interviews or focus groups, in addition to broadening data sources to include observations, class artifacts, documents, or other sources related to educational initiatives focused on educating children about digital safety. The examination of these initiatives would allow for data collection across multiple stakeholders, which would include teachers, students, parents, school administrators, and district technology leaders. Additionally, large-scale surveys would allow for researchers to examine the experiences, concerns, and efforts of multiple participants and see if there are commonalities among participants.

Conclusion

With the increase in student access to digital technology, digital safety actions are critical to keeping the children safe. The findings from this qualitative study from interviews with elementary school teachers have implications for fellow teachers, administrators, parents, and students. Research has identified several concerns that teachers have regarding elementary school children's digital safety (Stoilova et al., 2019). These concerns should be addressed by K-12 educators with actions taken to prevent future occurrences. Administrators should work towards providing technology infrastructure for filters, technology limits, and monitoring. Both in-service and pre-service teachers should be provided with professional development opportunities. Incorporating digital safety into teacher education courses will assist the teachers in keeping the elementary school students safe. Also, parent and community outreach will assist in keeping the children safe online. The elementary school children are "digitally vulnerable" and the findings call for the need for more research on how to keep the children "digitally safe."

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s11528-022-00803-z.

Funding This project was supported by the National Science Foundation Grant No. 2015554.

Data Availability Due to the IRB policy for this study, data cannot be shared from this study.

Declarations

Ethics Approval Institutional Research Board approval was received at the researchers institution.

Conflict of Interest The authors declare that there is no competing interests.

Permission to Reproduce Material Permission was obtained from Dr. Livingstone to use the 4Cs framework.

References

Aftab, P. (2000). *The parent's guide to protecting your children in cyberspace* (p. 330). McGraw-Hill.

Berger, P., & Wolling, J. (2019). They need more than technology-equipped schools: Teachers' practice of fostering students' digital protective skills. *Media and Communication, 7*(2), 137–147. https://doi.org/10.17645/mac.v7i2.1902

Buchanan, R. (2021). How to build a positive digital footprint for your school and for your students. In J. S. Brooks & A. Heffernan (Eds.), *The school leadership survival guide: What to do when things go wrong, how to learn from mistakes, and why you should prepare for the worst* (pp. 169–186). Information Age Publishing.

Buchanan, R., Southgate, E., Smith, S. P., Murray, T., & Noble, B. (2017). Post no photos, leave no trace: Children's digital footprint management strategies. *E-Learning and Digital Media, 14*(5), 275–290. https://doi.org/10.1177/2042753017751711

Burke, C., & Bloss, C. (2020). Social media surveillance in schools: Rethinking public health interventions in the digital age. *Journal of Medical Internet Research, 22*(11), e22612. https://doi.org/10.2196/22612

Couvillon, M. A., & Ilieva, V. (2011). Recommended practices: A review of schoolwide preventative programs and strategies on cyberbullying. *Preventing School Failure: Alternative Education for Children and Youth, 55*(2), 96–101. https://doi.org/10.1080/1045988X.2011.539461

DePaolis, K. J., & Williford, A. (2015). The nature and prevalence of cyber victimization among elementary school children. *Child & Youth Care Forum, 44*, 377–393.

Fardouly, J., Magson, N. R., Johnco, C. J., Oar, E. L., & Rapee, R. M. (2018). Parental control over time preadolescents spend on social media: Links with preadolescents' social media appearance comparisons and mental health. *Journal of Youth*

and Adolescence, 47, 1456–1468. https://doi.org/10.1007/s10964-018-0870-1

Hills, E. (2018). 2. A Survey on the Cybersecurity of K-12 Schools. https://digitalcommons.northgeorgia.edu/ngresearchconf/2018/Posters/9/

Hollandsworth, R., Donovan, J., & Welch, M. (2017). Digital citizenship: You can't go home again. *TechTrends, 61*, 524–530. https://doi.org/10.1007/s11528-017-0190-4

International Society for Technology in Education (ISTE) (2019). ISTE standards for educators. https://www.iste.org/standards/for-students

Jones, L. M., & Mitchell, K. J. (2016). Defining and measuring youth digital citizenship. *New media and society, 18*(9), 2063–2079. https://doi.org/10.1177/1461444815577797

Kahlke, R. M. (2014). Generic qualitative approaches: Pitfalls and benefits of methodological mixology. *International Journal of Qualitative Methods*, *13*(1), 37–52. https://journals.sagepub.com/doi/pdf/10.1177/160940691401300119

Kumar, P., Naik, S. M., Devkar, U. R., Chetty, M., Clegg, T. L., & Vitak, J. (2017). 'No telling passcodes out because they're private': Understanding children's mental models of privacy and security online. Proc. of ACM: Human-Computer Interaction, 1, CSCW, Article 64 (November 2017), 21 pages. https://doi.org/10.1145/3134699

Kumar, P. C., Chetty, M., Clegg, T. L., & Vitak, J. (2019). Privacy and security considerations for digital technology use in elementary schools. *In CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019,* Glasgow, *Scotland UK.*

Lester, T. M. (2018). *An investigation of cyber safety awareness among teachers and parents (Publication No. 10845057).* [Doctoral dissertation, Gardner-Webb University]. Proquest Dissertation Publishing.

Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying online risk to children. https://www.ssoar.info/ssoar/bitstream/handle/document/71817/ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf?sequence=4&isAllowed=y&lnkname=ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf

Mark, L. K., & Nguyen, T. T. (2017). An invitation to internet safety and ethics: School and family collaboration. *Journal of Invitational Theory and Practice, 23*, 62–75.

Martin, F., Gezer, T., & Wang, C. (2019). Educators' perceptions of student digital citizenship practices. *Computers in the Schools, 36*(4), 238–254. https://doi.org/10.1080/07380569.2019.1674621

Martin, F., Gezer, T., Anderson, J., Polly, D., & Wang, W. (2021). Examining parents perception on elementary school children digital safety. *Educational Media International, 58*(1), 60–77. https://doi.org/10.1080/09523987.2021.1908500

Martin, F., Gezer, T., Wang, W., Petty, T., & Wang, C. (2022). Examining K-12 educator experiences from digital citizenship professional development. *Journal of Research on Technology in Education, 54*(1), 143–160. https://doi.org/10.1080/15391523.2020.1815611

Merriam, S., & Tisdell, E. J. (2014). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey-Bass.

Percy, W. H., Kostere, K., & Kostere, S. (2015). Generic qualitative research in psychology. *The Qualitative Report, 20*(2), 76–85. https://doi.org/10.46743/2160-3715/2015.2097

Richards, D., Caldwell, P. H., & Go, H. (2015). Impact of social media on the health of children and young people. *Journal of Pediatrics and Child Health, 51*, 1152–1157.

Rideout, V., & Robb, M. B. (2019). *The common sense census: Media use by tweens and teens, 2019*. Common Sense Media.

Saldaña, J. (2021). *The coding manual for qualitative researchers*. Sage.

Shade, L. R., & Singh, R. (2016). "Honestly, we're not spying on kids": School surveillance of young people's social media. *Social Media + Society, 2*(4), 1–12. https://doi.org/10.1177/2056305116680005

Stoilova, M., Livingstone, S., & Nandagiri, R. (2019). Children's data and privacy online: Growing up in a digital age. https://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline

Strauss, A. L., & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Sage.

UN (United Nations) Committee on the Rights of the Child (2021). General Comment 25 on children's rights in relation to the digital environment. Geneva: UN. https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

Vega, V., & Robb, M. B. (2019). *The Common Sense census: Inside the 21st-century classroom*. Common Sense Media. https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-educator-census-inside-the-21st-century-classroom_1.pdf

Young, R., Tully, M., & Ramirez, M. (2017). School administrator perceptions of cyberbullying facilitators and barriers to preventive action. *Health Education and Behavior, 44*(3), 476–484.