2020

Risk Communication Framework for Parental Control in the Digital World

Alotaibi, Moneerah N

Copyright Statement

UNIVERSITY OF PLYMOUTH

Risk Communication Framework for Parental Control in the Digital World

By

Moneerah Nawar Alotaibi

A thesis submitted to the University of Plymouth in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Engineering, Computing and Mathematics

August 2020

Acknowledgements

First and foremost, I give honour and praise to Allah the Almighty for giving me strength and helping me to complete this PhD, which is an important stage of my life.

In addition, I wish to express my heartfelt appreciation to my beloved father (may Allah have mercy upon him) and mother for their kindness and for providing me with an abundance of love and support, and I ask Allah to bless her with good health. In this same vein, I am grateful to my sisters and brothers for their endless support and help. Very deep and special thanks also go to my children, my daughter and son, who have unfailingly given endless patience and love.

Of course, I would like to express my honest gratitude and appreciation to my Director of Studies, Professor Steven Furnell, for providing me with a wealth of support and help to complete my PhD work. I have really appreciated his support, encouragement and understanding in difficult situations. I also wish to thank my second supervisor, Dr Maria Papadaki, and third supervisor, Dr Shirley Atkinson, for their time and support.

I would also like to express my thanks to all the participants for taking part in the study from the University of Plymouth Freshlings Nursery, the Suzanne Sparrow Plymouth Language School, and St Andrew's Primary School.

Lastly, I acknowledge with gratitude the government of Saudi Arabia and Shaqra University for granting me the scholarship and sponsoring my undertaking of this PhD programme.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee. Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment. Relevant scientific seminars and conferences were regularly attended at which work was often presented and several papers prepared for publication.

This study was financed with the aid of a scholarship from the Kingdom of Saudi Arabia - Royal Embassy of Saudi Arabia Cultural Bureau in London.

Word count of the main body of thesis: 35,550

Signed Moneerah Alotaibi

Date 26 / 08 / 2020

Abstract

Risk Communication Framework for Parental Control in the Digital World

Moneerah Alotaibi

The Internet is growing rapidly and is becoming an essential part of children's lives. Internet use has many benefits for learning, participation, creativity, entertainment and communication. Along with such benefits, however, Internet use might expose children to a wide range of online risks. Some of those risks, such as bullying, exposure to pornography, and sexual exploitation, are known in the offline world but there are also new ones, such as the invasion of personal data and privacy, geolocation tracking, sexual messaging and harassment. Unfortunately, the existing mechanisms for protecting children online are ineffective. The parental controls currently available focus on monitoring and restrictive functions to reduce potential online risks, which might not satisfy the expectations of young people who want unrestricted freedom to use the Internet. Parental controls also demonstrate shortcomings in increasing parents' awareness of the risks that their children may encounter. Parents not only need to be aware of their children's online activities, but also to understand and mitigate the potential risks associated with their children's online activities. Young people might engage in online behaviours that expose them to risk, although not all risk leads to harm. Therefore, parental controls should improve parents' awareness of the potential security risks related to their children's online activities, so that they can support their children's use of the Internet, enhance their opportunities and help them develop the coping skills to deal with potential risk.

The present research suggests applying a risk communication mechanism to parental controls to raise the security awareness for parents and children in order to help them make safe decisions and reduce online risks. Firstly, this research proposes a risk assessment model that assess the risk levels of children's online activities in order to warn parents and children about them in an individualised, timely, and continuous way. The proposed system also provides appropriate protection responses to avoid those risks. Secondly, a prototype system has been designed and developed to simulate the proposed system and provide a clear image of its functionalities and how it works. After implementing the prototype system, it was important to have parents evaluate its usability and usefulness. The participants were able to use the system and were satisfied in terms of its overall appearance and the functions provided. They agreed and prefer to use the system in real life. It can also be stated that the overall feedback from the participants regarding the proposed system was very encouraging and positive.

Table of Contents

Copyright Statement 1
Acknowledgements 3
Author's Declaration 4
Abstract 5
Table of Contents 6
List of Tables 9
List of Figures 11
Chapter 1: Introduction 13
1.1 Introduction 13
1.2 Aims and objectives 16
1.3 Thesis structure 17
Chapter 2: Internet use by children and young people 19
2.1 Children's Internet access 19
2.2 Children's Internet use 21
2.3 Online risks 24
2.3.1 Classification of online risks 24
2.3.2 Children's exposure to online risks and harm 26
2.4 Parental awareness and mediation of children's Internet use 32
2.5 Conclusion 35
Chapter 3: Review of the literature on parental controls and attempts at awareness raising among children 36
3.1 Overview of existing parental control software 36
A comparison of parental control applications against the essential criteria 43
3.2 Overview of existing information security awareness initiatives for children and parents 45
3.3 Conclusion 49
Chapter 4: Risk communication framework for parental control 50
4.1 Risk assessment and communication approaches to promoting online safety about specific security issues 50
4.2 Framework for applying risk communication in parental controls 52
4.2.1 Risk assessment model for children's Internet use 55
4.2.2 Protection responses 77
4.3 Simulation of system reaction with different scenarios 81
4.3.1 Scenario related to real-world stories of children's participation in interactive situations and exposure to contact and conduct risks 82

4.3.2 Scenario related to real-world stories of children's exposure to content risks and computer/Interne risks 89
4.4 Conclusion 92
Chapter 5: Proof-of-concept prototype 93
5.1 Prototype system implementation overview 93
5.1.1 Assigning general protection responses 97
5.1.2 Assessing the risk level of questionable activities and customising the protection responses 99
5.1.3 Assessing the activities involved on a specific platform (application category) 102
5.1.4 Simulated alert 104
5.2 Conclusion 105
Chapter 6: Prototype system evaluation 106
6.1 Prototype system evaluation methodology 106
6.1.1 Research method 106
6.1.2 Data collection methods 109
6.1.3 Research participants 111
6.1.4 Pilot test 112
6.1.5 Data analysis 115
6.2 Prototype system evaluation findings 116
6.2.1 Participants and their children's Internet use data 116
6.2.2 Participants' attitudes and performance with the system 131
6.2.3 Task completion times 138
6.2.4 Parents' level of satisfaction with the system 139
6.3 Discussion 146
Chapter 7: Conclusions and future work 150
7.1 Achievements of the research 150
7.2 Limitations of the research 153
7.3 Suggestions and scope for future work 155
7.4 Importance of protecting children online 156
References 158
Publications 164
Appendices 165
Appendix A: Ethical approval letter, research information sheet, consent form, and invitation 165
Appendix B: Task scenarios 171
Appendix C: Pre-survey questionnaire 174
Appendix D: Post-survey questionnaire 183

Appendix E: Participants' assessment of the risk level of their children's online activities in different age groups 185

List of Tables

Table 1 Daily online activities, 2019 (Smahel et al. 2020) 22
Table 2: Existing parental control applications and the essential functions 44
Table 3 A review of information security awareness initiatives for children and parents 48
Table 4: Risk levels of online activities 59
Table 5: Weight values of risk factors 61
Table 6: Descriptive values for the age factor 62
Table 7: SDQ for children aged 4-17 63
Table 8: Sensation-seeking measure 64
Table 9: Internet experience results for children in different age groups 65
Table 10: Internet experience factor values 66
Table 11: Descriptive values for the location factor 68
Table 12: Descriptive values for the device type factor 69
Table 13: Descriptive values for the frequency factor 70
Table 14: Average time per day spent with different applications by US youth, 2015 71
Table 15: Average time young people spent with different applications per day 71
Table 16: Descriptive values for the duration factor 72
Table 17: Probability values 76
Table 18: Risk matrix for different risky activities 77
Table 19: Protection responses and their main characteristics 80
Table 20: System's responses to different risky activities of chatting with strangers in social networks 86
Table 21: System's response to exposure to inappropriate content 91
Table 22: Usability scenarios 107
Table 23: Participants' children's Internet usage 117
Table 24: Participants' children's online activities by age 119
Table 25: Participants' assessment of the risk levels of online activities 122
Table 26: Activities impact assessment by participants 124
Table 27: Participants' level of concern about their children's Internet use at different ages 125
Table 28: Reasons parents were not concerned about their children's Internet use 126
Table 29: Participants' concerns about their children's online activities 127
Table 30: Participants' concerns about each activity (parents not generally concerned) 128
Table 31: Parental mediation used by participants 129
Table 32: Parental mediations used by participants with different concern levels 129
Table 33: Parental mediation used with children in different age groups 130
Table 34: Participants' use of existing parental controls 130

Table 35: Participants’ completion of tasks 1 and 2 132
Table 36: Parents’ performance of tasks 1 and 2 136
Table 37: Time taken for tasks to be completed 138
Table 38: Participants' satisfaction with the system design and functionalities..... 142
Table 39: Participants' comments about the system..... 144

List of Figures

Figure 1: Estimated weekly hours of internet use by age (2009, 2011, 2014, 2017 and 2018) (Ofcom 2019a) 13
Figure 2: Devices used by children: 2009,2012,2017,2018, and 2019 (Ofcom 2019b) 14
Figure 3: Devices “mostly” used by children to go online at home, by age: 2012, 2017.2018 and 2019 20
Figure 4: Tablet and smartphone ownership by age of child: 2019 21
Figure 5: Internet use by age: children aged 8-11, 11-14 and teenagers aged 14-17 years old 23
Figure 6: Estimated weekly hours spent with different activities, by age: 2019 24
Figure 7: Comparison of children’s risk experiences in 2010 and 2014 27
Figure 8: Online experiences that have bothered children, comparing mobile and non-mobile Internet users 28
Figure 9: Children's experience of contact and content risks in 2017,2018, and 2019 (Ofcom, 2019) 29
Figure 10: children’s exposure to online risks increase with increased time spent online 29
Figure 11: Incidence of parents allowing their children to go bed with a mobile 33
Figure 12: Parental agreement with difficulties to control their children's screen time 33
Figure 13: Parents' awareness of parental control services and software 34
Figure 14: Screen Time feature 37
Figure 15: Android parental control feature 38
Figure 16: Screenshot of Net Nanny 39
Figure 17: Screenshot of time controls on individual applications 40
Figure 18: Screenshot of Norton Family Premier 41
Figure 19: Screenshot of Kaspersky Safe Kids 42
Figure 20: Screenshot of Mobicip 43
Figure 21: Screenshot of the Childnet website 46
Figure 22 Screenshot of UK Safer Internet Centre 46
Figure 23: Screenshot of the Thinkuknow website 47
Figure 24: Screenshot of the Internet Matters 48
Figure 25: Risk matrix for smartphones 51
Figure 26: Risk communication framework for parents and children 54
Figure 27: Main interface of the system 95
Figure 28: Main interface for managing a child's account (Emily) 96
Figure 29: Assigning general protection responses for low, medium, and high risk events 98
Figure 30: Assessing the risk level of questionable activities and customising the protection responses 99

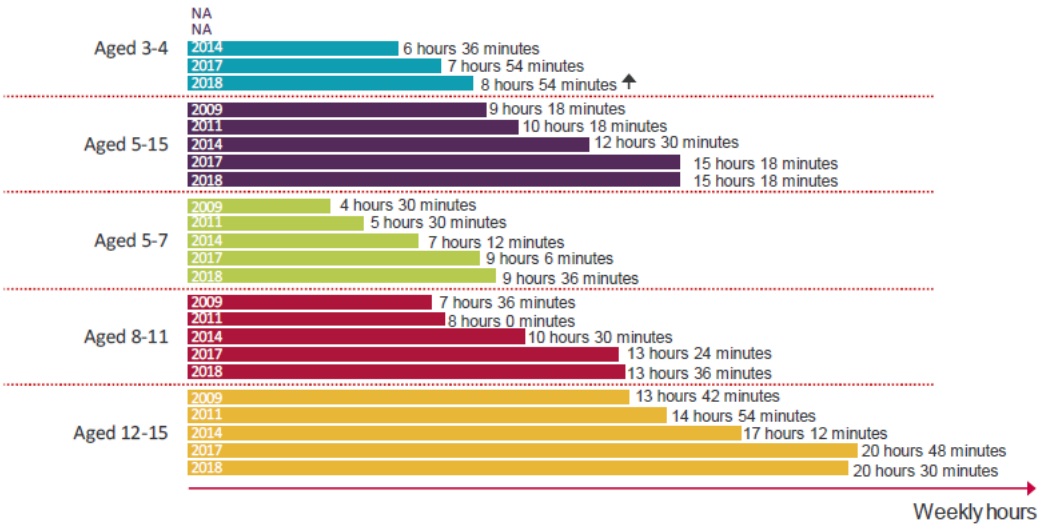
Figure 31: Assessing the risk level of ‘Accessing inappropriate content’ and assigning protection responses 101
Figure 32: Managing web activities 103
Figure 33: Simulated alert 105
Figure 34: Changes to the main interface for managing the child's account 113
Figure 35: Changes to the interface for managing risky activities 114
Figure 36: Participants’ assessment of the risk levels related to online activities 121
Figure 37: Participants' responses regarding the clarity of the system concept 140
Figure 38: Participants' satisfaction with the system design and functionalities 141
Figure 39: System interfaces after changes in response to parents’ feedback 147

Chapter 1: Introduction

This chapter provides an introduction to the research context and an overview of the main issues related to the subject of study. The aims and objectives of the research are then presented, followed by a brief summary of each chapter.

1.1 Introduction

The Internet is growing rapidly and becoming an essential part of children's lives. The use of the Internet is deemed important, especially for learning, communication, entertainment and play purposes. Young people spent more hours online, Ofcom find that the estimated time spent online by children has increased markedly since 2017 for all age groups, as shown in Figure 1 (Ofcom 2019a).

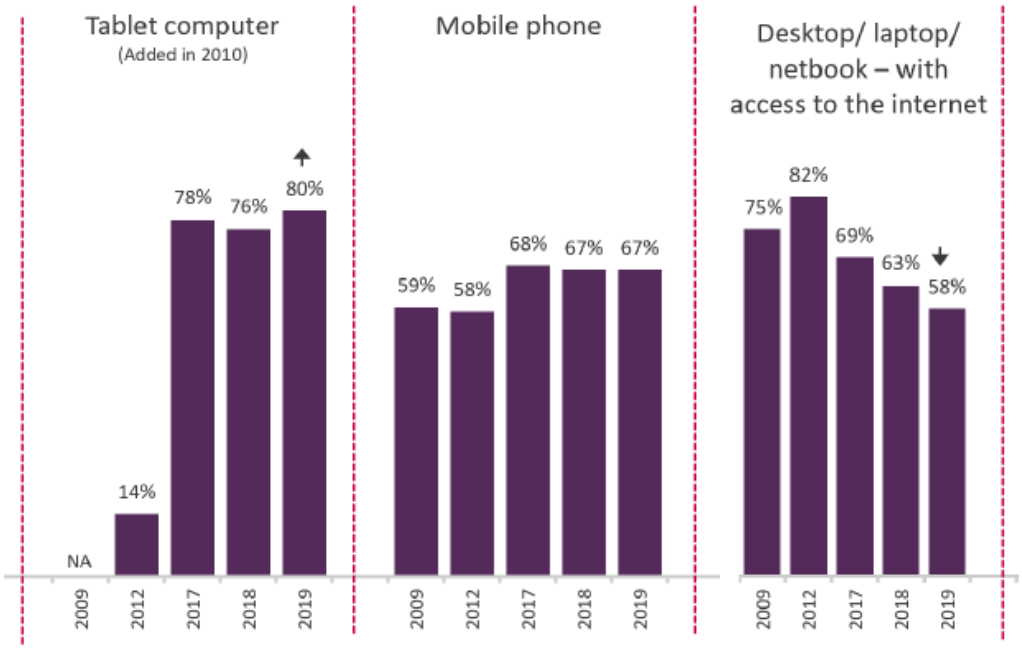


(Ofcom 2019a)

Figure 1: Estimated weekly hours of internet use by age (2009, 2011, 2014, 2017 and 2018)

Furthermore, advances in digital technology have changed children's Internet use, from using desktop computers and laptops to various mobile devices, such as smartphones and tablets that have expanded children's online activities (Livingstone, Haddon, et al. 2014). The use of

mobile phone and tablet increased for all age groups while use of desktop/ laptop/ netbook decreased since 2017, as shown in Figure 2 (Ofcom 2019b).



(Ofcom 2019b)

Figure 2: Devices used by children: 2009,2012,2017,2018, and 2019

Also, EU Kids Research also published a similar result about children's Internet use in 2019. The research found that the majority of children used smartphone to access the Internet. The number of children going online from their mobile phones ranged from 31% to only 2% in 2010, while the percentage of children using a phone or smartphone to access the internet in all comparable countries has risen, ranged from 65% to 86%. Also, the time that children report spend on the Internet almost doubled compared to the findings of the EU Kids Online survey in 2010 that was ranged from about 1 hour to 2 hours in 2010 (Smahel et al. 2020)

Despite the benefits, however, use of the Internet might expose young people to an array of online risks, such as exposure to harmful or offensive content, inappropriate contacts (online harassment and bullying), advertising and commercial exploitation, misuse of personal data and privacy issues. Furthermore, online risks are rising fast with the increase in children's Internet

use via personalised and mobile devices (Livingstone, Mascheroni, et al. 2014) (Mascheroni and Ólafsson 2014). According to EU Kids Online reports, the percentage of children who reported that they had been bothered online varied between 6% and 25% across comparable countries in the EU Kids Online survey 2010, while the percentage of children who reported such experiences was higher in most of the countries in EU Kids Online 2020 report (between 7% and 45%) (Smahel et al. 2020). Also, according to Ofcom report 2020, 81% Of children aged 12-15 had potentially harmful online experiences and the experiences relating to interactions with other people or content are much higher amongst children, (74% relating to interaction with other people/content, 39% relating to data/privacy, 27% relating to hacking/security) (Ofcom 2020).

Furthermore, young people are not always cautious when they use the Internet, and they engaged in risky online activities (e.g., sharing personal information) without being aware of the consequent threats (Annansingh and Veli 2016)(Sithira and Nguwi 2014). Some children are also unaware of how safeguarding their online behaviour such as changing privacy setting (Ofcom 2020). Thus, there is a need to protect children and make them aware of online risks and how to cope with them.

In addition, some parents have a low level of awareness of their children's online activities and Internet risks, some parents did not monitor their children Internet use (Symons et al. 2016) (Martin et al. 2018). Some parents do not always understand the risks their children may encounter. They help their children to create accounts in social networks without knowing that they are putting their children at risk (Association 2014). There are parental control software are developed to support parents in protecting their children. However, a minority of parents use parental control applications for blocking, filtering and monitoring their children's Internet use (Anderson 2016) (Smahel et al. 2020) (Ofcom 2019b). Furthermore, parents often have difficulty in working with parental control software, for example, some parents did not know how to change the parental control settings (AV-Comparatives, 2014) (Pons-Salvador et al.

2018). Also, some parents find parental controls are inadequate and restrictive (AV-Comparatives, 2014) (Ofcom 2019b). Existing parental controls focus on monitoring children Internet use and restricting that use. Parents need, therefore, to be more involved in and aware of their children's day-to-day Internet activities and the potential risks in order to support their children's use of the Internet and protect them.

Therefore, improving parental controls is an important area of research in order to safeguard children online. The research aims to provide an easy to use, flexible and adaptable system that will raise awareness about the potential risks associated with children's online activities and give parents a granular level of control to manage their children's Internet use and help them make informed decisions.

1.2 Aims and objectives

This research reviews children's Internet access and use. It also provides an overview of associated online risks and identifies the main factors that influence children's online experiences. Furthermore, the study investigates the current methods for protecting young people online and identifies the gaps in those approaches. The study aims to improve current parental controls by proposing a flexible system that uses a risk communication mechanism to raise the security awareness of children and parents, and to give parents more control.

In order to achieve the above aims, this project pursued the following objectives:

- Investigate children's online activities, the threats and risks associated with them, and parental mediation used for protecting children online.
- Develop a state-of-the-art understanding of the current methods for safeguarding young people, which involves the investigation of existing information security awareness initiatives and parental control software available for parents.
- Propose a risk communication framework for parental control that helps parents and children to be aware of the online risks associated with children's Internet use, as well as a

risk assessment model that estimates the risk levels of children's online activities and identifies the protection responses that should be taken with different risk levels.

- Develop and implement a proof of concept of the proposed framework, which will monitor and assess the risk levels of children's online activities and make different protection responses depending on the risk level.
- Evaluate the usability and usefulness of the proposed system among parents.

1.3 Thesis structure

The thesis is organised into the following chapters in order to address the above-mentioned objectives.

Chapter 2 looks at young people's online experiences. Children use of the Internet and mobile technologies exposed them to a wide range of online risks. Young people engaged in harmful online activities without being aware of the consequent threats. Also, some parents are unaware of their children's online activities and Internet risks. As a result, there are some parental control software and information security awareness initiatives are developed for protecting children online.

Chapter 3 provides an overview of the approaches currently used for safeguarding young people online including existing parental control software that enable parents to monitor and restrict children Internet use, and information security awareness initiatives that provide resources for raising awareness about Internet safety for parents and young people; and also investigates the obstacles and issues relating to those approaches. Thus, the security awareness should be integrated with parental controls through using risk communication mechanism to provide a flexible system that can predict the potential risks of children's online activities in real time and raise awareness about these risks and means of safeguarding for parents and children.

Chapter 4 presents a review of the risk communication approaches used for promoting Internet safety and raising awareness of different security issues of users. Thus, a risk communication

framework for managing children's Internet use and raising awareness of potential risks is developed. Also, the risk assessment model for assessing risk levels of children's online activities and protection response options are proposed. So, parents and children could understand the potential risks of online activities and make informed decisions.

Chapter 5 presents a prototype system that simulates the proposed system and provides a clear image of its functionalities and how it works. The chapter describes the system's interfaces and details the process of risk assessment of children's online activities and the customisation of protection responses.

Chapter 6 discusses the evaluation methodology used for assessing the usability and usefulness of the system, which includes the experiment procedure, and research participants. The chapter then presents the findings of the evaluation process after analysing the data collected through a survey questionnaire and direct observation undertaken during the experiment. The experiment results provides indication about the participants' acceptance and satisfaction about the system usability and usefulness.

Finally, Chapter 7 presents the main conclusions from the research, highlighting the principal achievements and limitations of the work. The chapter also presents suggestions for potential future improvement that need to be undertaken.

Chapter 2: Internet use by children and young people

The Internet is growing rapidly and is becoming an essential part of children's lives. Internet use has many benefits for learning, participation, creativity, entertainment and communication. Along with the benefits, however, the Internet use might expose children to a wide range of online risks, some of which are known in the offline world, such as bullying, pornography, sexual exploitation, and the viewing of inappropriate content, scenes of violence and suffering. There are also new risks, such as the invasion of personal data and privacy, geolocation tracking, sexual messaging and harassment (Ólafsson, Livingstone, and Haddon 2014). The following section of this chapter presents a review of children's Internet use and the devices used. Threats and risks associated with children's Internet use are then outlined.

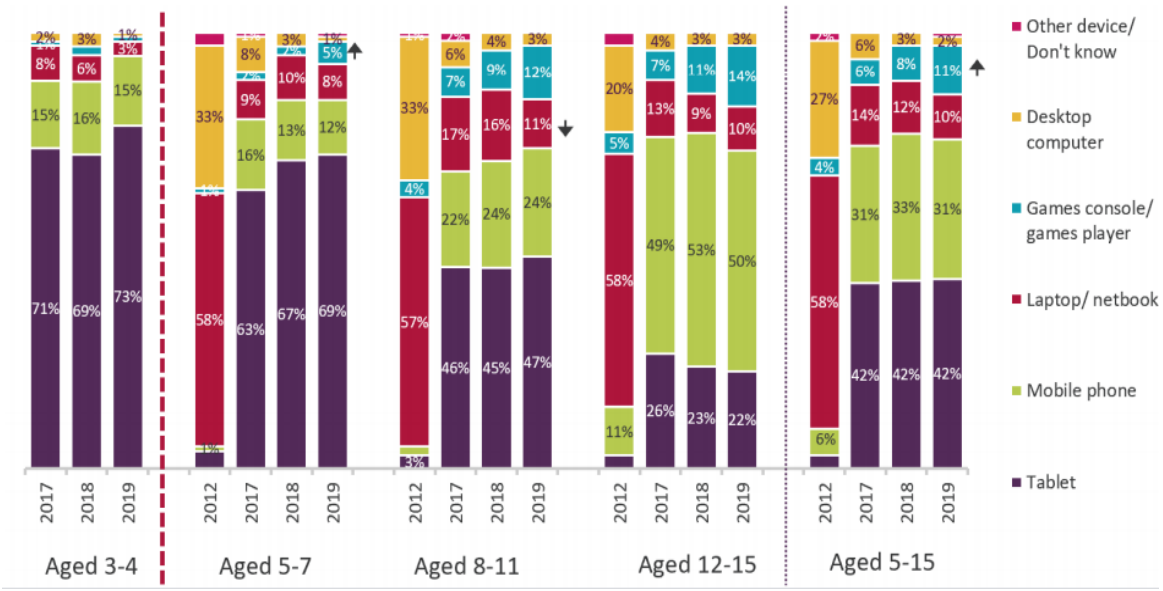
2.1 Children's Internet access

The Internet and mobile technologies have presented a world of opportunities for children to learn and participate in society. The Internet represents an educational resource, as well as a platform for social interaction and entertainment. Young people engage in a range of online activities.

Furthermore, the advent of smart, mobile devices with touch-screen and networking capabilities has expanded Internet use among children by providing 'anywhere, anytime' accessibility. The speed, ease of use, portability and instant accessibility of mobile platforms have increased their use by children. Children have also changed their mode of Internet access, from using fixed computers, laptops and traditional devices to various mobile devices, such as smartphones and tablets.

Ofcom research conducted some studies to seek Internet use among young people. According to Ofcom study that was conducted through 2,343 interviews with parents of 5-15s and children aged 8-15 along with 900 interviews with parents of children aged 3-4, there has been a

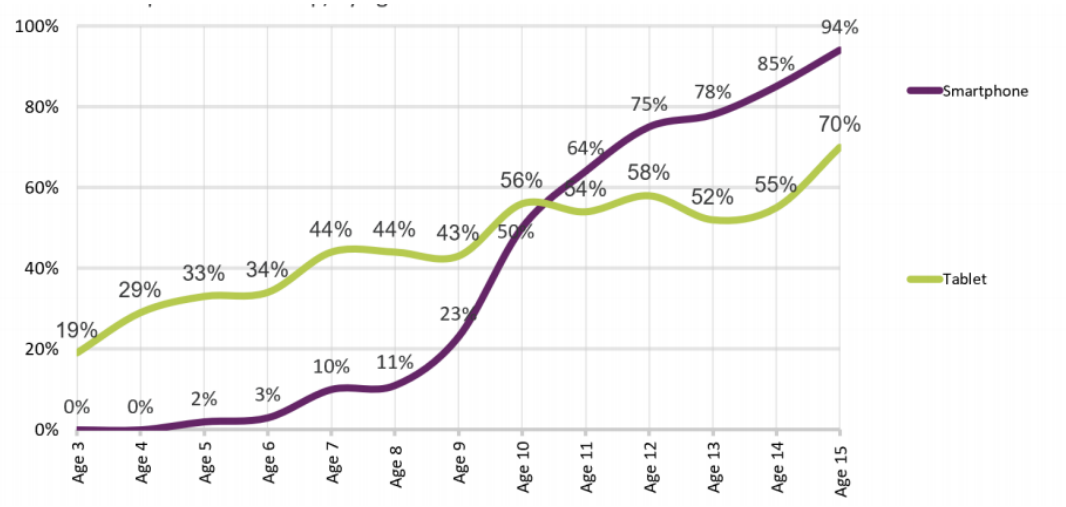
significant increase in use of mobile devices by children of all ages, as shown in Figure 3. The number of children who mostly access the Internet via a laptop or netbook and PC has decreased. By contrast, the number of children who are now mainly using an alternative device to access the Internet has increased, with tablets (42%) and mobiles (31%) being the most common devices (Ofcom 2019b).



(Ofcom 2019b)

Figure 3: Devices "mostly" used by children to go online at home, by age: 2012, 2017.2018 and 2019

Several studies also show that younger children are more likely to use tablets for many activities, and older children are more likely to use their mobile phones (Catshill Learning Partnerships, Education technology association, and Naace 2017) (Ofcom 2019b). According to Ofcom study, children under the age 10 are more likely to own a tablet, while after this age children are likely to have a smartphone, as shown in Figure 4 (Ofcom 2019b).



(Ofcom, 2019)

Figure 4: Tablet and smartphone ownership by age of child: 2019

Also, EU Kids Online research; which is a multinational research network funded as part of the European Council's Safer Internet Programme; conducted a survey with children aged 9-16 to seeks and improve knowledge of European children's online activities, risks and safety. The study shows that older children are more likely to access the internet daily from their smartphones than younger children (81% vs 35%). Also, younger children were likely to spend 114 minutes on the internet every day, while the older children tend to spend more time on the internet daily around 229 minutes (Smahel et al. 2020).

2.2 Children's Internet use

Children use the Internet for entertainment, education, and communicating with their friends. Young people engage in a variety of online activities, which have been categorised as "hanging out", "geeking out" and just "messing around". "Hanging out" involves children interacting with others by browsing social networks, instant messaging, and phone and video conversations. "Geeking out" involves children doing specific activities for interest, such as gaming or video and music file sharing. Finally, "messing around" describes media engagement in which young people are learning and becoming serious about something. It also includes the

use of search words to find information about interesting issues and experimenting, for example by using photo and video editing tools (Ito et al. 2010).

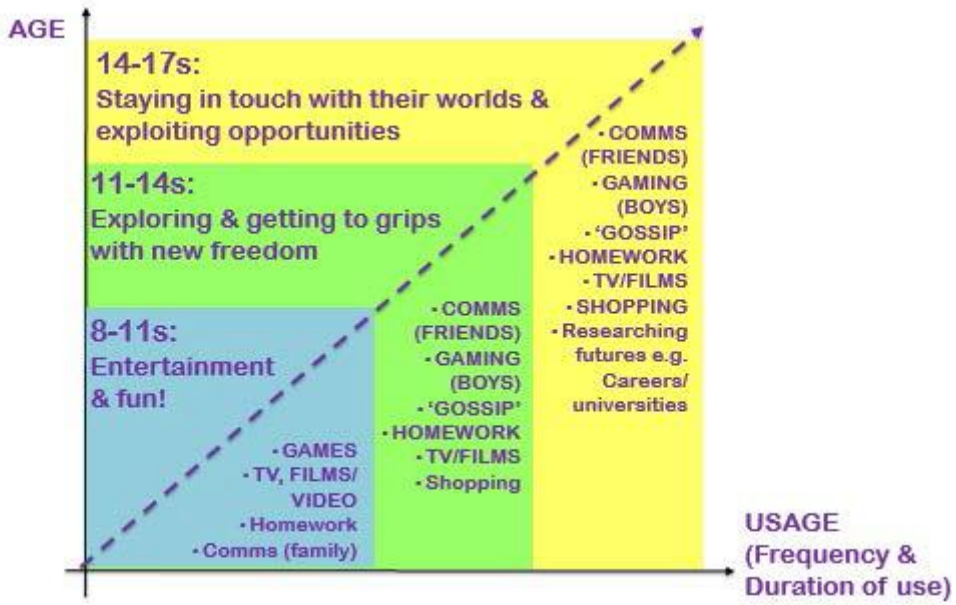
Also, EU Kids Online research show that children's most common online activities are watching videos, listening to music, communicating with friends and family, visiting a social networking site and playing online games, as shown in Table 1 (Smahel et al. 2020).

Table 1 Daily online activities, 2019 (Smahel et al. 2020)

Online activities	Percentage of children who did the activity
Watch video clips	65
Listen to music online	65
Communicate with family or friends	61
Visit a social network site	54
Play online games	44
Use the internet for schoolwork	31
Brows for things to buy or see what things cost	20
Look for news online	19

Furthermore, Internet use among young people changes with age. Younger children tended to use the Internet for much shorter periods of time and their favourite activities were watching television and playing games. Older children used the Internet primarily to communicate with their families and others (Third et al., 2014). Also, Ofcom study grouped young people were into age bands based on their Internet use and attitudes of each, as shown in Figure 5. Younger children are those aged 8-11, "tweens" refers to those aged 11-14, and teenagers are aged 14-17 years old. The research found that children aged 8-11 used the Internet for entertainment and that games tended to predominate in their online activities. Tablets were the main device and were used as personal TV sets to watch favourite programmes and films on YouTube. "Tweens"

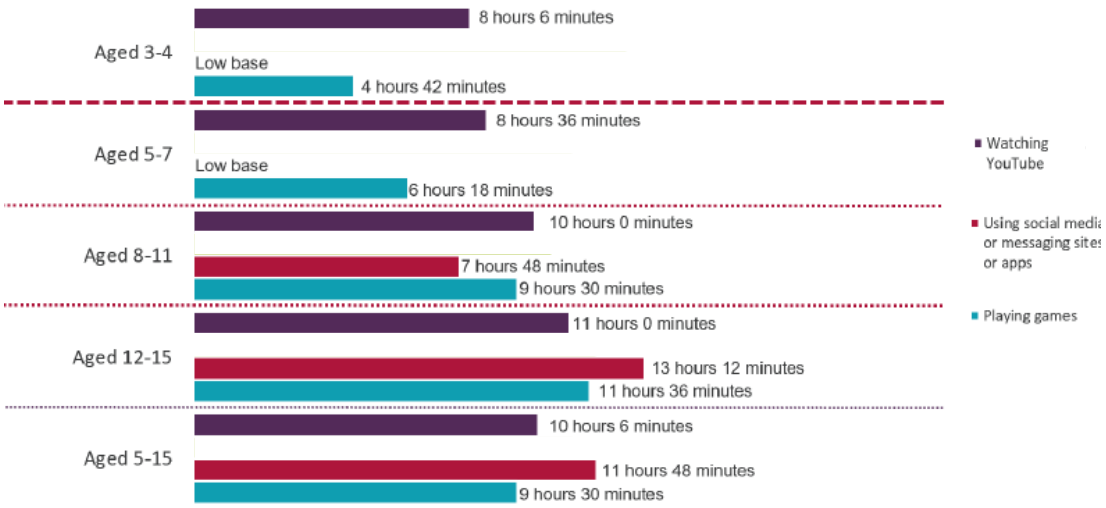
(those aged 11-14) used the Internet for gaming, communication, shopping, and creativity apps. They accessed the Internet using their devices, usually their phone. The most common activities for older teenagers aged 14-17 were communication and using social networking and messaging platforms. They also followed celebrities and brands via social media and used the Internet for schoolwork, shopping and gaming. Young people in this age band accessed the Internet via their mobiles, and the amount of time they spent on those devices was greater than was the case with the younger children (Ofcom 2014a).



(Ofcom, 2014)

Figure 5: Internet use by age: children aged 8-11, 11-14 and teenagers aged 14-17 years old

Ofcom Research also published a similar result about children's Internet use in 2019, as shown in Figure 6 (Ofcom, 2019). The research showed that the children's online activities varied by age. Younger children spent the most time watching YouTube, while older children spent the most time using social media (Ofcom 2019b). In general, children engaged in different online activities at different ages. As the children's age increased, they also took part in a wider range of online activities.



(Ofcom 2019b)

Figure 6: Estimated weekly hours spent with different activities, by age: 2019

2.3 Online risks

The Internet has become a primary foundation in children's lives for the acquisition of knowledge and for entertainment. Children's Internet use could expose them to online risks. The following sections present the classification of online risks and children's experiences of negative events online.

2.3.1 Classification of online risks

Several classifications of online risks for children have been developed, and they all separate between risks related to harmful content and those to harmful interactions. The EU Kids Online report presents classification of online risks based on the role of the child: content threats (Child as recipient of an inappropriate content), contact threats (Child as participant in an interaction mostly driven by adults), and conduct threats (Child as actor/ initiator in an interaction) (ACMA 2008). Also, the Australian Communications and Media Authority (ACMA) involves content risks, communication risks, and e-security risks such as viruses and spam that are not included by the EU Kids Online report (Livingstone and Haddon 2009). These threats: content threats,

contact threats, conduct threats, and computer/Internet threats, are presented in more detail in turn in the following sections.

2.3.1.1 Content threats

The Internet hosts a lot of content that is easily accessible to all users. It enables a wide variety of information to spread quickly and freely across the world. Some of the content is inappropriate for all ages, and children may be exposed to it either by actively searching it or by accident. Content threats involve the exposure of children to inappropriate material that might be harmful, such as adult/abusive material, improper content, racist or biased information (S Livingstone and Haddon 2009).

2.3.1.2 Contact threats

Contact threats involve a variety of risky situations, such as those related to sexuality (grooming, sexting), psychology (cyberbullying), and privacy threats (privacy loss) (Livingstone and Haddon 2009). Children mainly experience contact risks via the Internet through social network sites and chat rooms.

Sexuality-related threats include grooming and sexting. Grooming involves adults' attempts to establish an emotional relationship with a child with the aim of sexually abusing him/her. Sexting involves exchanging sexual messages or other content, such as photos or videos, using the Internet.

Cyberbullying involves the abusive use of communication platforms to harass, threaten, or insult others. Children may become victims of online cyberbullying when threatening or insulting mails are sent to them, through verbal abuse in chat rooms or social networks, or by the dissemination of offensive photographs.

Privacy loss involves inappropriate use of children's sensitive or private information. Children might pass their personal details such as their age, name, address and phone number, either during a transaction with a service provider or during their contacts with other people. The

potential result of privacy loss could be unwelcome offline contact, harassment and abuse (Magkos et al. 2014) (Valcke et al. 2011).

2.3.1.3 Conduct threats

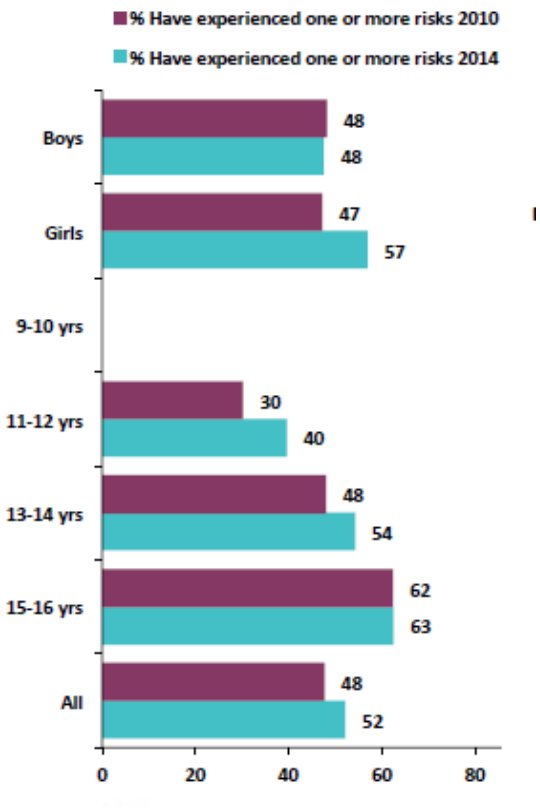
Conduct threats include a child being involved in activities such as bullying or harassing other children, or creating and uploading inappropriate or harmful material. Conduct threats usually come from young people themselves (Livingstone and Haddon 2009) (Hartikainen et al. 2015).

2.3.1.4 Computer/Internet threats

There are various security threats for all users of the Internet and these also apply to children. Computer/Internet threats include malware, phishing, viruses, spyware, identity theft and Internet addiction. Internet addiction is the excessive use of computers/Internet, whereby a child may have a poor ability to restrain and limit his/her Internet use (Magkos et al. 2014) (Hartikainen et al. 2015).

2.3.2 Children's exposure to online risks and harm

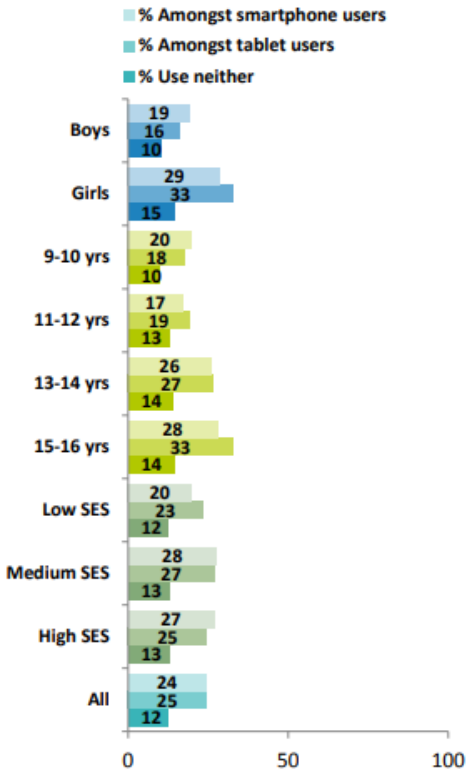
Advances in technologies with increased use of the Internet by young people could increase online risks and harm. At the time this PhD research began, there are some studies reported the situation of children online experiences and the increase online risks. For example, the EU Kids Online Survey conducted in 2010 and the Net Children Go Mobile survey conducted in 2014 showed that the percentage of children who had encountered at least one online risk increased from 48% in 2010 to 52% in 2014, as shown in Figure 7. Also, the percentage of children who reported being bothered by online experiences increased from 13% in 2010 to 17% in 2014 (Livingstone et al. 2014).



(Livingstone et al. 2014)

Figure 7: Comparison of children's risk experiences in 2010 and 2014

In addition, the speed and ease of mobile access have also increased the risks encountered by children, as children can immediately distribute and share inappropriate content without thinking about the possible negative consequences of their actions. Net Children Go Mobile report shows that the increase in smartphone and tablet use is linked to a rise in the number and types of online risks. It finds that 24% of children who used smartphones daily had been bothered by their online experiences, 25% of tablet users had had online experiences that bothered them, but only 12% of the children who used neither smartphones nor tablets had had such experiences, as shown in Figure 8 (Mascheroni and Ólafsson 2014).



(Mascheroni and Ólafsson 2014)

Figure 8: Online experiences that have bothered children, comparing mobile and non-mobile Internet users

During the period when the PhD research is running, further studies have been conducted to show the current situation of children' exposure to online risks. For example, Ofcom report in 2019 finds that experience of content risks (e.g., seeing sexual or scary content) and contact risks (e.g., communicating with unknown people) have increased in 2019, as shown in Figure 9 (Ofcom 2019b). Ofcom research also published a similar result about online risk experiences in 2020, most of children aged 12-15 (81%) had potentially harmful online experiences. Also, the study shows that children's exposure to online risks increase with increased time spent online especially in weekend, as shown in Figure 10 (Ofcom 2020). The experiences relating to interactions with other people or content are much higher amongst children (74% relating to interaction with other people/content (e.g., unwelcome friend, bullying, hate speech, pornographic content, self-harm), 39% relating to data/privacy (e.g., spam emails, data collection for commercial use), 27% relating to hacking/security (e.g., scams, viruses)). Also,

the study find that bullying impacts children the most and was very annoying/ upsetting (51%), as well as hate speech, content promoting self-harm and viruses (42%, 40%, and 46% respectively) (Ofcom 2020).

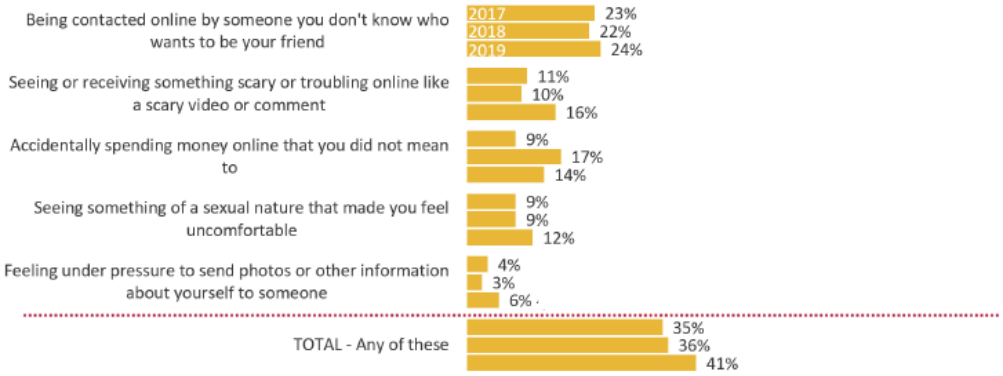


Figure 9: Children's experience of contact and content risks in 2017,2018, and 2019 (Ofcom, 2019)

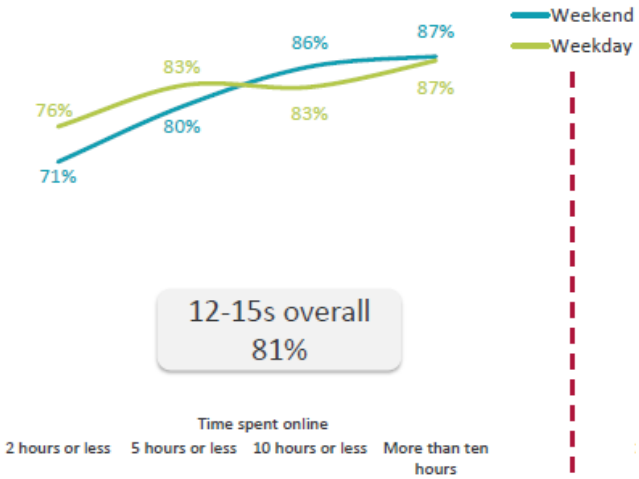


Figure 10: children's exposure to online risks increase with increased time spent online

Also, EU Kids report finds that content and contact risk were the most often experiences reported, and the number of children who reported negative experiences in 2019 was higher (between 7% and 45%) than in 2010 (between 6% and 25%). Children exposed to different harmful content and the most often reported harmful content were hate messages (Ave = 17%) and sexual images (Ave = 14%). Also, children exposed to different types of risks such as cyberbullying and sexting. Children exposed to more contact risk than conduct risks. Children were usually involved in any risky behaviour as a victim more than as an aggressor. They

involved in aggressive behaviour as a victim more than as an aggressor (23% vs 14%). In relation to sexting, sending sexual messages is less common than receiving sexual messages (6% vs 22%). Also, contacting unknown people is a common experience (Ave = 37%), while meeting new people face to face is a less common experience among children (Ave = 16%). Other risks related to personal data misuse and privacy were less common and reported by fewer than 15% of the children (Smahel et al. 2020).Children exposed to different types of risks, , children also differ in their feeling and responses to risk experiences, the EU Kids study finds that most of the children victimised online were upset (80%) while a fifth report no harm (20%). Also, most of the children who saw some sexual image report no impact, while 38% of the children were upset. Furthermore, the study finds that older children aged 15-16 report more negative online experiences than younger children aged 9-11 (34% vs 20%), and young children are more upset from experience than older children (Smahel et al. 2020). Furthermore, children with more psychological difficulties were more likely to encounter risk and harm online (Livingstone and Smith 2014) (Oksanen et al., n.d.). Psychological difficulties may lead to higher risk-taking behaviour in the online context. Livingstone et al (2011) found that 34% of children who had psychological difficulties reported more online risks and more harm (Livingstone, Görzig, Ólafsson 2011).

Young people are not always cautious when using online services, and they involved in harmful online activities without being aware of the consequent threats (Annansingh and Veli 2016)(Sithira and Nguwi 2014). Also, some children are confident online in terms of their knowledge and skills but intentionally or unintentionally engage in risky online behaviour without understanding the consequences (Scott 2016). Research has shown that social networks are the most common source for most potential risks and harms (Ofcom 2020). Children engaged in a high level of unsafe behaviour on social network sites, such as chatting with strangers, sharing personal information with them, or agreeing to meet them in person without being aware of the consequent threats. Children might conduct these risky communications

because they find it easier to be themselves online and to talk about different matters online than offline (Smahel et al. 2020). Drevin and Drevin found that young people imagine that Facebook is secure and 48% of them have met someone new online and 42% have met someone in person through Facebook (Drevin and Drevin 2013). Furthermore, most children show private information on their SNS profiles, 76% of children were showed a photograph of their face, 83% showed their last name, 11% of children gave their phone number, and 58% showed their school (Livingstone, Haddon, Vincent, Mascheroni, and Ólafsson 2014).

Also, the number of children who communicate with unknown people and send personal information or a photo or video of themselves to unknown people are increased in 2016, and some children reported that getting followers was more important to them than keeping their information private. Thus, there is the potential to be exposed to risk on social media if children focus on acquiring and accepting followers or comments, particularly if this is at the expense of the child's privacy (Ofcom 2016). Furthermore, some young people are also unaware of how safeguarding their online behaviour. According to Ofcom report, 22% of young people did not know how change privacy setting, and this is percentage decreased with increasing age and higher levels of internet confidence. Also, 71% of young people did not report online harm, and 25% of them did not report harmful content because they hadn't seen anything harm to report and 17% did not find it was bad enough, while 12% did not know what to do (Ofcom 2020).

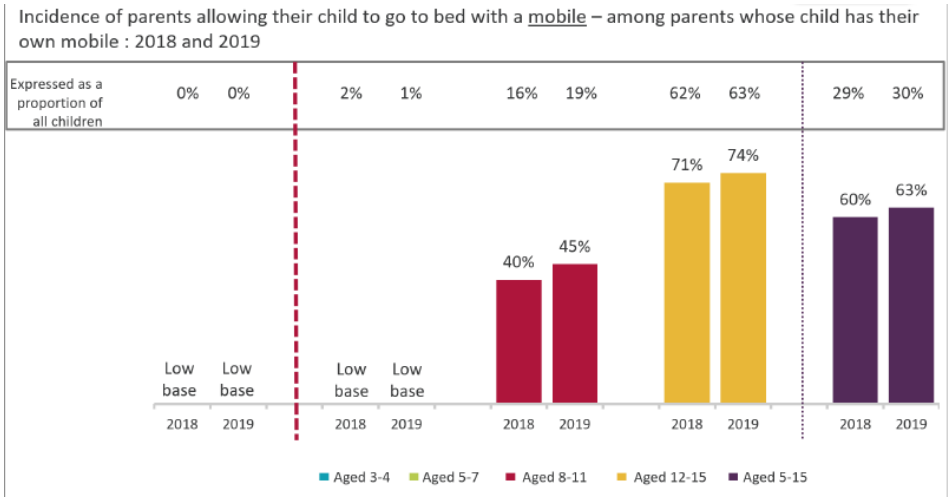
Furthermore, some young children use social networks despite the age limits for using these platforms. According to EU Kids report, 28% of children aged 9-11 have used social networks (Smahel et al. 2020). Also, another study find that 17% of children started using social networks at age nine or younger, 40% accepted friend requests from unknown people (Martin et al. 2018).

Overall, there is a need for protecting children online and raise awareness about the implications of their online activities. There are some factors could be used to assess the probability of child's exposure to online risks such as child's age, child's experience and psychological

characteristics, and factors related to child's internet access and use. older children could be more vulnerable to online risks due to their participation in a greater number of different types of online activities that might exposure them to more online risks. Also, children's use of mobiles devices and spending too much time on the Internet could increase exposure to online risks. In addition, child's awareness and his/her psychological characteristics could affect child's Internet experience and promote online risk-taking behaviour. Therefore, it is important and useful to consider harm and the individual factors of the child as a criterion for predicting and assessing the risk level of child's Internet use in order to protect the children and define the right actions to intervene and raise children awareness of online risks and means of safeguarding against them.

2.4 Parental awareness and mediation of children's Internet use

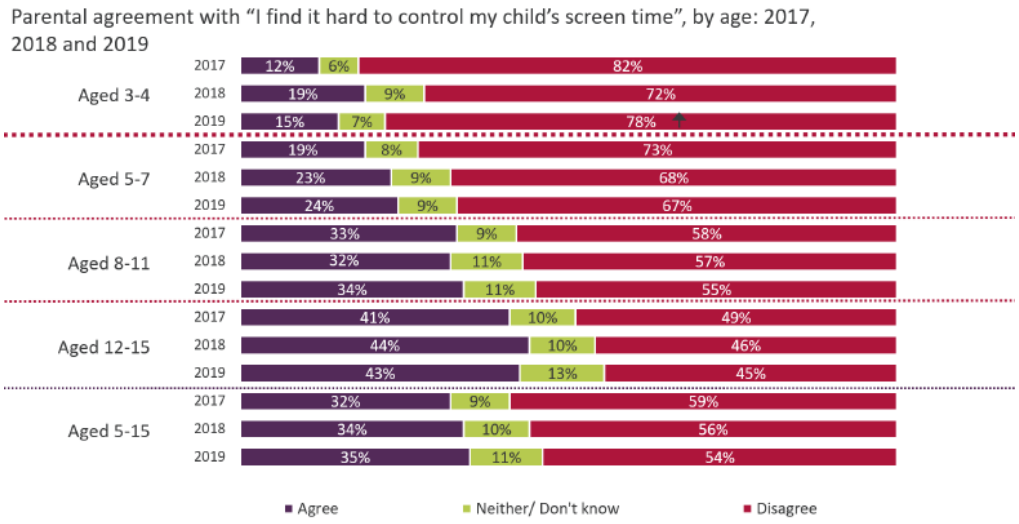
Some parents have a low level of awareness of Internet risks and their children's online activities (Symons et al. 2016). Some parents help their children to create accounts in social networks without knowing that they are putting them at risk (Association 2014). Furthermore, Martin found that some parents (40%) did not monitor their children's social networks use (Martin et al. 2018). Also, Ofcom report finds that most of parents allow their children to go to bed with their mobile in 2019 and that was more than in 2018, as shown in Figure 11 (Ofcom 2019b). In addition, only a small proportion of parents restrict their children Internet use and set some rules, for example, they do not allow their children to use web or phone cameras (16%), download content (12%) or use a social networking sites (16%). Some parents prefer advising their children on how to use the Internet safely (69%)., but some children ignore their parents' advice about how to use the Internet (46%) (Smahel et al. 2020).



(Ofcom,2019)

Figure 11: Incidence of parents allowing their children to go bed with a mobile

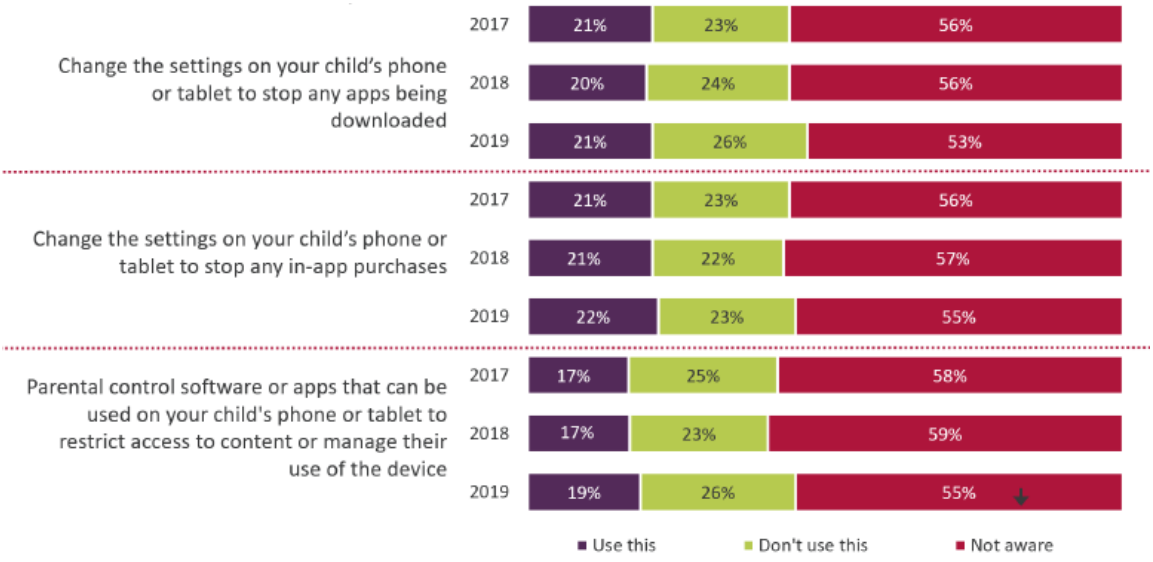
Also, some parents find difficulties in control their child's screen time especially when children get older. The number of parents who find difficulties in controlling their children Internet use is increased, as shown in Figure 12 (Ofcom 2019b).



(Ofcom 2019b)

Figure 12: Parental agreement with difficulties to control their children's screen time

In addition, more than half of parents are unaware of parental control software, and around half of parents who are aware of parental control software did not use it, as shown in Figure 13 (Ofcom 2019b).



(Ofcom 2019b)

Figure 13: Parents' awareness of parental control services and software

Also, Anderson finds that a few parents use parental control applications for blocking, filtering and monitoring their children's Internet use (39%) (Anderson 2016). Also, EU Kids finds similar results about parents' use of parental control software, a minority of parents use parental controls (Ave = 22% and less). Also, parental controls are used with younger children more than with older children. (Smahel et al. 2020).

Furthermore, parents often have difficulty in working with parental control software (AV-Comparatives 2014). Pons-Salvador et al. (2018) find that a half of parents did not know how to set up content filters or parental controls (57.9% of parents did not know how to change the parental control settings, 40.2% did not knew how to block pop-ups and spam). Also, parents find parental controls are inadequate and restrictive focusing on blocking that could be overblocking (blocks content that should not be blocked) or underblocking (permits content that should not be permitted) (AV-Comparatives 2014) (Ofcom 2019b). So, parental controls should be more flexible, easy to use and able to raise awareness about the potential risks of children's online activities for parents and help them to make informed decisions and protect children online.

2.5 Conclusion

This chapter focused on children's online practices and experiences. The increased Internet use by children could expose them to online risks and harm. Also, there are some factors could increase exposure to online risk such as child's age and psychological characteristics, and also child's internet use. Children engaged in a wider range of online activities and they are not always cautious when they are using the Internet. They engaged in harmful online activities without being aware of the consequent threat. Furthermore, some parents are unaware of their children's online activities and Internet risks. Furthermore, a minority of parents use parental control, and some parents find parental control software are too restrictive. So, this chapter highlights the parental control software should be flexible, and help parents to manage their children' online activities. So, the parental control should take into account the factors that increase the probability of child's exposure to online risks in order to be able to predict and assess the potential risks, and then raise awareness about these risks and help parents to take the conscious decision and encourage safe behaviour.

So, the next chapter reviews the existing mechanisms for protecting children online including parental control software and information security awareness initiatives against these requirements and investigate obstacles and issues relating to those approaches in more detail.

Chapter 3: Review of the literature on parental controls and attempts at awareness raising among children

Safe Internet use by young people is being promoted by governments and the industry that developed certain strategies and tools to keep children safe. There are technical solutions to help parents safeguard their children's online experiences, such as parental controls that involve monitoring and blocking tools. In addition, there are initiatives to raise awareness for young people and parents about Internet safety. This chapter reviews the parental control software and information security awareness initiatives in order to explore obstacles and issues relating to these approaches.

3.1 Overview of existing parental control software

Parental control features have been developed as services or applications that parents can use to keep their children safe. There are parental control functions that are embedded into a device operating system (OS), such as built-in parental control features (Screen Time feature) in Apple iOS, as displayed in Figure 14. The features mean that parents can monitor how much time their children spend on various applications and control the device used by their children. It provides functions such as limiting the time of device use and application use, and content and privacy restrictions on inappropriate content, purchases, downloads, and privacy (Apple 2020).

Figure 14: Screen Time feature

Android devices also have built-in parental control features. Google's Family Link offers features for parents to monitor how much time their children spend on different applications, as displayed in Figure 15. It also enables parents to set restrictions, such as a time limit for device and application use, and restrict content that can be downloaded or purchased from Google Play based on maturity level (Google Play Help n.d.).

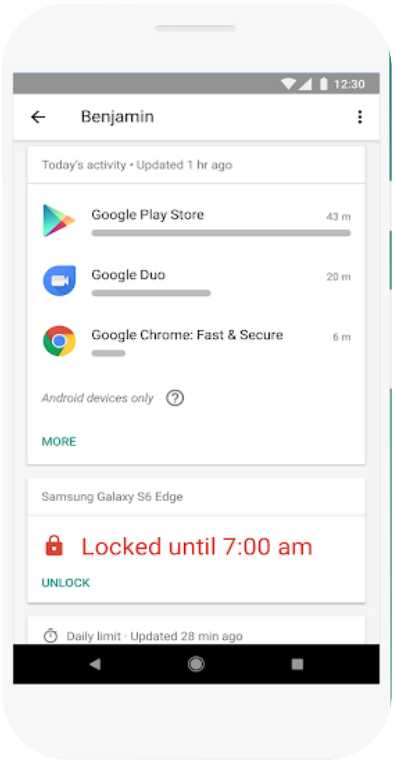


Figure 15: Android parental control feature

The parental control features above work on specific devices (Apple devices, Android devices) and it might be easy to evade the control by re-installing the OS. There are also parental controls provided by routers that offer functions such as access restrictions. Providers, such as O2 and EE, offer services for voice-and-data communication that include parental control features. These features restrict children's web access to a limited number of sites that are suitable for them. Overall, the majority of feature developers consider parental control to be an additional feature and not a main aspect of the development process.

In addition, there are standalone parental control applications. According to recent reviews, the best examples of parental control software are as follows: Net Nanny, Qustodio, Norton Family Premier, Kaspersky Safe Kids, and Mobicip (Ellis 2020) (Rubenking and Moore 2019) (Wagenseil 2020) (Johnston 2019).

Net Nanny enables parents to monitor and restrict child usage such as limit time, filter, and block unsafe materials, as shown in Figure 16. In addition, Net Nanny has a dynamic filter that

checks each website and advertisement in real time to determine if it is appropriate for the child. It can also detect inappropriate activities such as visiting an inappropriate content and send an alert to the parent, allowing the latter to approve or override the blocked page and allow the child access. Also, it can detect dangerous or inappropriate chat in social network, and send an alert to parents ("Net Nanny Parental Control Overview" n.d.) ("Net Nanny Parental Control Overview" n.d.).

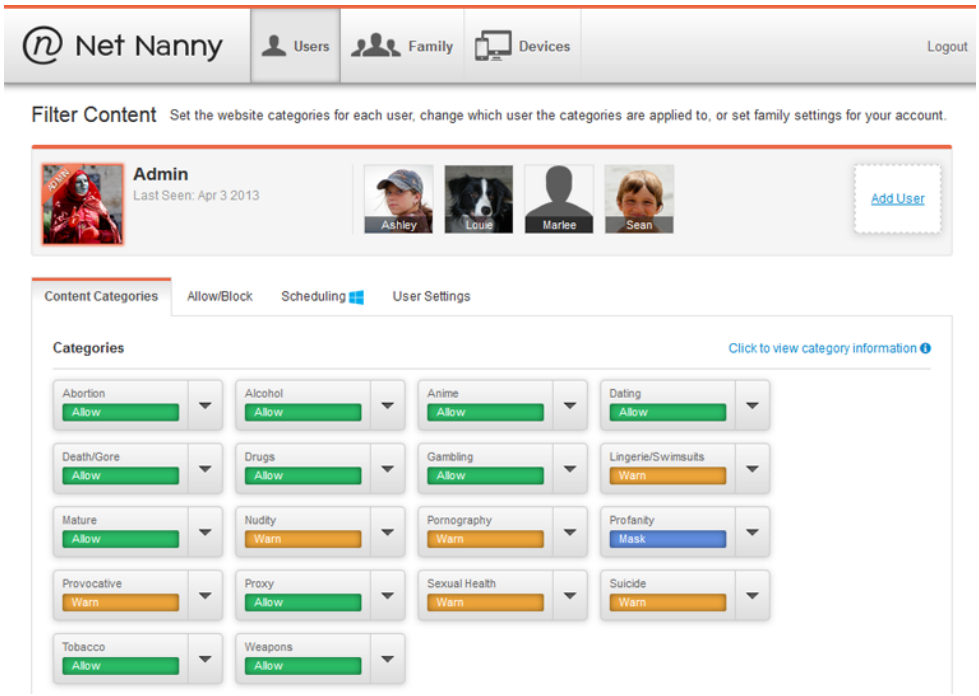


Figure 16: Screenshot of Net Nanny

Qustodio enables parents to monitor and restrict child's Internet use such as filter and block inappropriate content, and limit time on individual applications and games, as shown in Figure 17. It also monitors children's social network activities (it only tracks Facebook), and alerts parents to new social contacts and identifies those to whom the child talks or texts most frequently, and allows to block contacts. It can also monitor the time a child spends on each application, such as a particular website or social network. Thus, Qustodio helps parents who are concerned that their child spends too much time on a specific application or communicates too often with specific people (Qustodio, n.d.) ("The Internet's Best Free Parental Control App" n.d.) (Hall 2016).

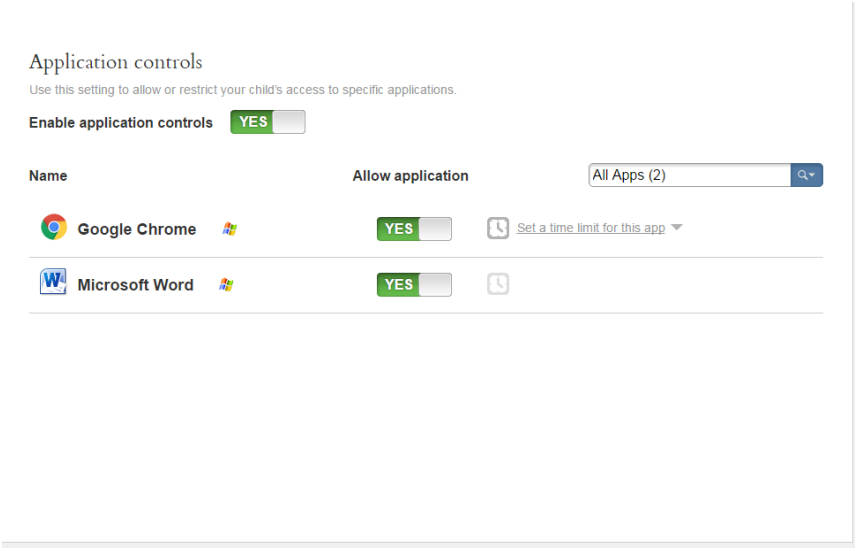


Figure 17: Screenshot of time controls on individual applications

Norton Family Premier is a parental monitoring service that offers parents the ability to monitor and restrict child's activities such as filter content, and block specific applications and location-tracking features, as shown in Figure 18. It can limit the time spent online on a device, but cannot place time limits on specific applications. It also sends an email when the child attempts to access a blocked website (Rubenking 2018) ("Parental Control Software - Norton Family" n.d.) (Hall 2016).

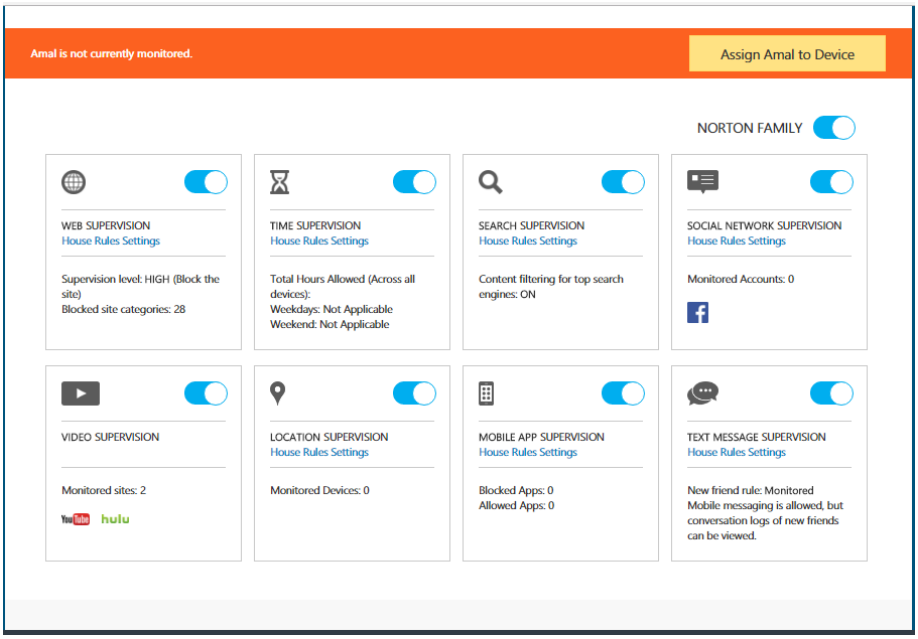


Figure 18: Screenshot of Norton Family Premier

Kaspersky Safe Kids enables parents to monitor and restrict child's Internet use such as limiting the time of application use, filtering content, and location tracking, as shown in Figure 19. Parents can also manage their children's social media use (it only tracks Facebook and VK), and receive real-time alerts if they visit inappropriate websites (Kaspersky Safe Kids, n.d.) (Ellis 2020) (Rubenking and Moore 2019) (Pustovalova 2016).

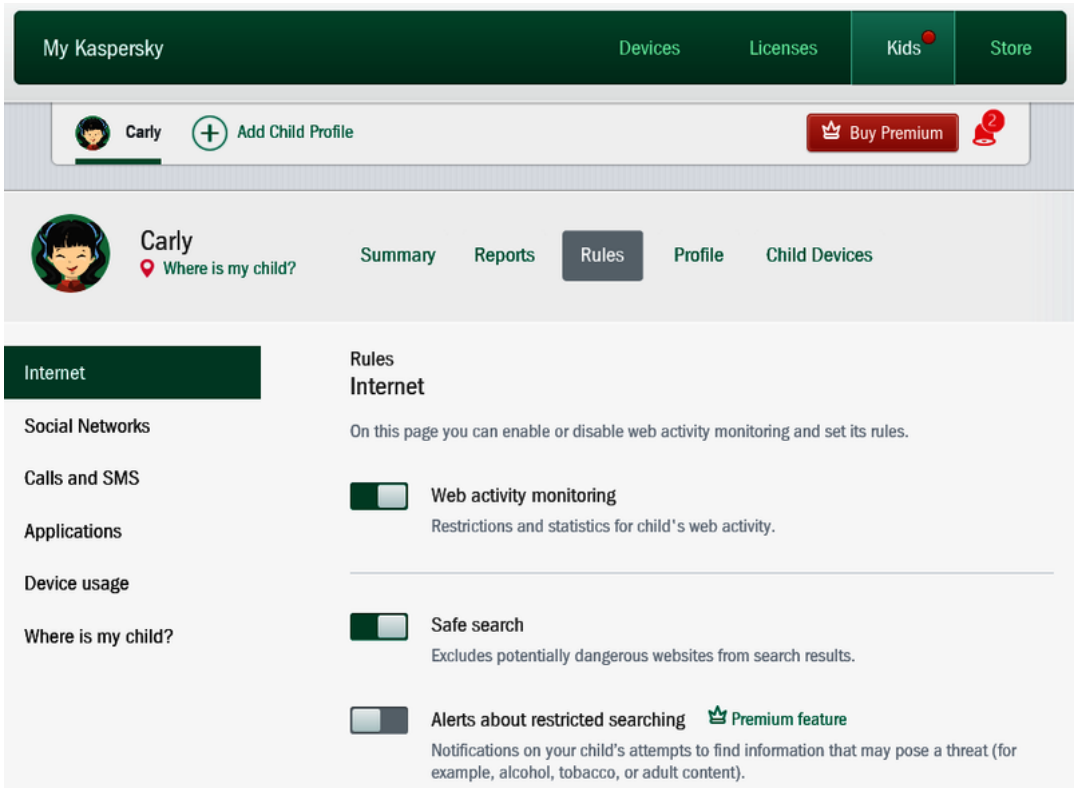


Figure 19: Screenshot of Kaspersky Safe Kids

Mobicip enables parents to monitor a child's activities, filter and block inappropriate content, track location, block individual apps (such as Facebook and Snapchat), and block an entire device, as shown in Figure 20. Mobicip can also monitor a child's conversations on social media platforms and send alerts by email to parents if the chatting involves high-risk keywords and phrases, such as "home alone" or "do not tell", or if the child tries to share personal information, including full name, date of birth and phone numbers. It also sends alerts to parents when a child attempts to access blocked content (Johnston 2019) (Mobicip, n.d.).

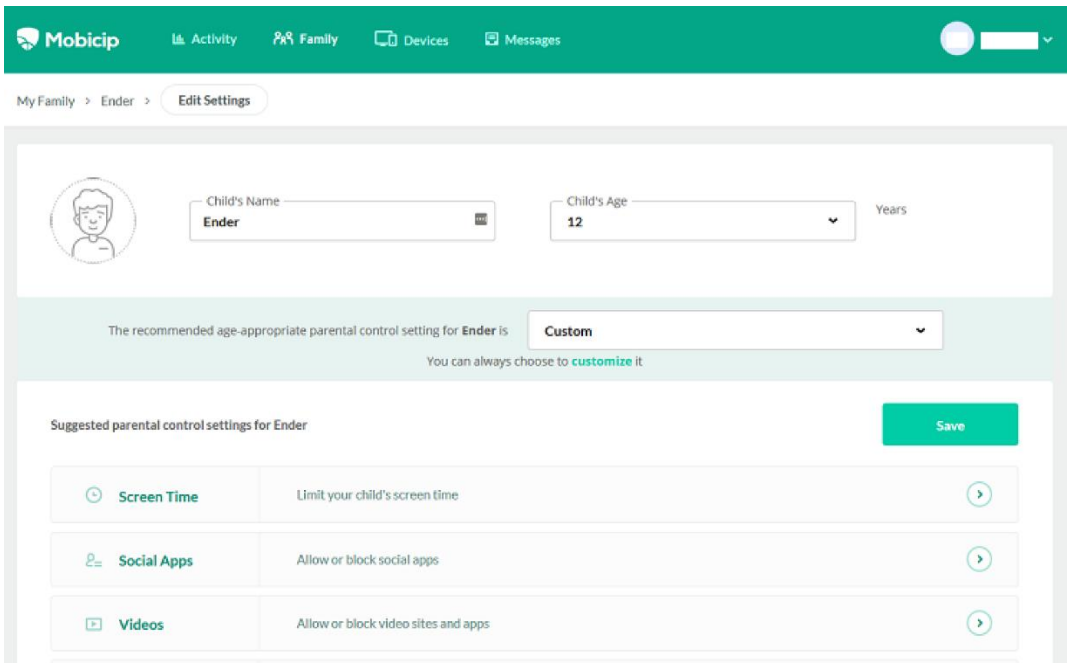


Figure 20: Screenshot of Mobicip

A comparison of parental control applications against the essential criteria

In order to protect children online, parental control should be flexible and able to predict the potential risks of children online activities and raise awareness about the potential risks of that use for parents and children and enable informed decisions, as we mentioned in the previous section 2.3.2. So, the following Table 2 presented the existing parental control and the important features should be available in the parental control applications.

Table 2: Existing parental control applications and the essential functions

Features	Parental control applications				
	Net Nanny	**Kaspersky Safe Kids**	**Mobicip**	**Qustodio**	**Norton Family Premier**
Monitoring online activities and predicting risk level					
Monitoring online search	✓	✓	✓	✓	✓
Monitoring websites visited	✓	✓	✓	✓	✓
Monitoring Email	✓	×	✓	×	×
Monitoring Social networking	✓	✓	✓	✓	✓
Assessing risk level of activity	×	×	×	×	×
Protection responses					
Alert parent					
Sends alerts on banned sites	✓	✓	✓	✓	✓
Sends alerts when detecting harmful language used in chat or SNS	✓	×	✓	×	✓
Sends alerts of new social contacts	×		×	✓	×
Raising awareness					
Raising a customized awareness for parents	×	×	×	×	×
Raising a customized awareness for children	×	×	×	×	×
Filtering and blocking					
Website filtering and blocking	✓	✓	✓	✓	✓
Online search filtering	✓	✓	✓	✓	✓
Application blocking	✓	✓	✓	✓	✓
Games filtering	✓	✓	✓	✓	×
Time control					
Time limiting for Internet use or device	✓	✓	✓	✓	✓
Time limiting for applications	×	✓	×	✓	×

The existing parental controls focus on monitoring children's Internet use, restricting and blocking that use. Monitoring capabilities include monitoring the websites visited, the words and phrases typed into a search engine, email, and activities on social networks. The filtering and blocking feature involves blocking applications and inappropriate websites (i.e., blocking blacklists that are implemented by means of URLs, keywords, and age differentiation in accordance with the age level defined in the software). Also, the existing parental control applications offer alerting services for specific inappropriate activities such as accessing inappropriate content or inappropriate chatting, or adding a new contact. Also, existing parental control applications differ in their abilities to limit time, which might involve limiting time for device use or for individual application use. However, existing parental control applications do not assess the risk level of children's online activities and raise awareness for parents and children about the potential risks and how to deal with them. So, none of parental control applications match all the criteria that we believe are important in protecting children online.

3.2 Overview of existing information security awareness initiatives for children and parents

There have been attempts to improve parents and young people's awareness of information security. There are several organisations that offer e-safety resources to help protect young people and educate them in how to stay safe, such as Childnet, Thinkuknow, the UK Safer Internet Centre, and Internet Matters. Childnet International is a non-profit organisation that produces a range of resources, such as leaflets, books and films for young people, parents, carers, and teachers (http://www.childnet.com/resources), as shown in Figure 21. The resources for young people are divided into two groups: primary and secondary. Primary student resources provide advice, quizzes, books, films and some external resources. There are interactive games that helps to educate children and offers the opportunity to experience online risks and asks them to make decisions.

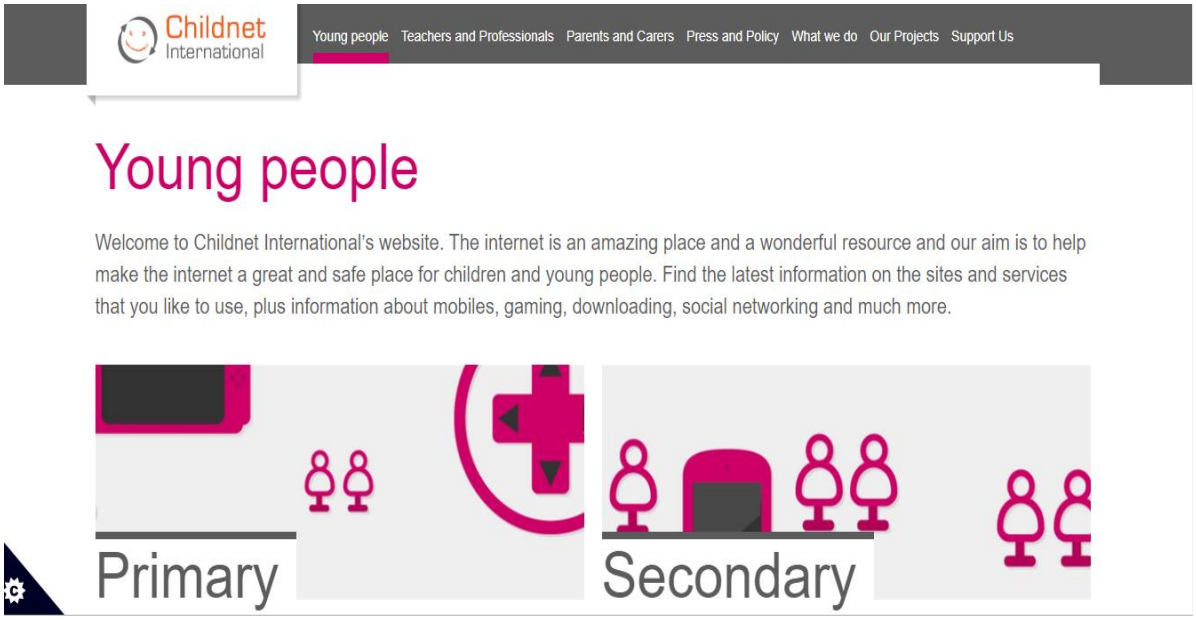


Figure 21: Screenshot of the Childnet website

There is also the UK Safer Internet Centre, which was developed by three organisations: Childnet International, the South West Grid for Learning (SWGfL), and the Internet Watch Foundation. This centre aims to raise awareness about Internet safety by organising events such as Safer Internet Day and providing information resources for primary and secondary pupils and parents/carers (http://www.saferInternet.org.uk), as shown in Figure 22. It provides a lesson plan, quick activities, films, storybooks, and external resources to help children stay safe on the Internet.

Figure 22 Screenshot of UK Safer Internet Centre

In addition, Thinkuknow provided by the Child Exploitation and Online Protection command (CEOP) provides a range of information resources about online safety for teachers, parents, and young people (https://www.thinkuknow.co.uk/), as shown in Figure 23. Resources include advice, activities, and videos. They are categorised on the basis of different age groups (5-7, 8-10, 11-13, and 14+). The resources for children aged 5-7 include videos contain stories featuring cartoon characters and dialogue concerning the safe use of computers. The resources aimed at children aged 8-10 include videos, games, and advice with more detail than is given to the younger age group. The resources for the two older age groups provide advice about common issues facing children of those ages and a video with characters from real life.

Figure 23: Screenshot of the Thinkuknow website

The Internet Matters gives information for parents on the online issues of cyberbullying, inappropriate content, online pornography, online reputation, online grooming, sexting, self-harm and radicalisation (https://www.internetmatters.org/), as shown in Figure 24. It also has instructions for parents for setting up appropriate parental controls and filters.

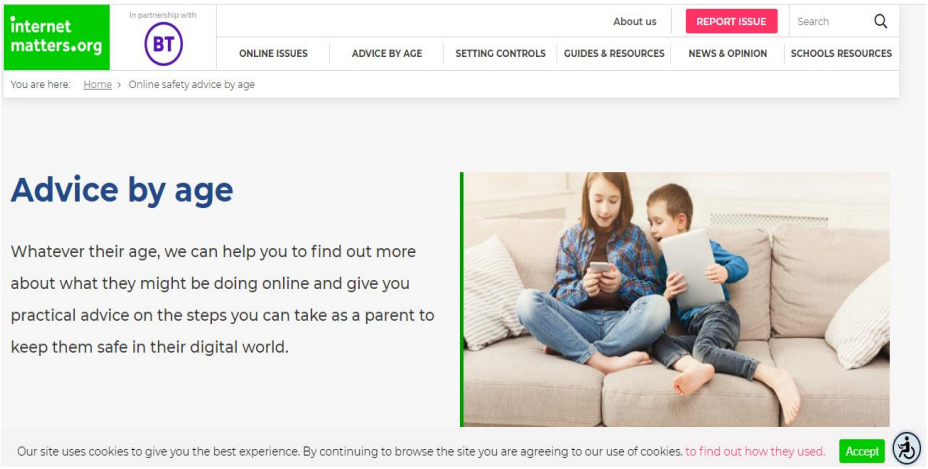


Figure 24: Screenshot of the Internet Matters

A review of these resources are presented in the following Table 3. Overall, these initiatives provides different resources to raise awareness about Internet safety for parents and young people at different age, and are available in different websites. However, many of children and parents are still unaware of the security risks when children go online (Annansingh and Veli 2016). Thus, parents and children should be aware of threats related to their use of the Internet and how to keep children safe online. .

Table 3 A review of information security awareness initiatives for children and parents

	Childnet	**Thinkuknow**	**The UK Safer Internet Centre**	**Internet Matters**
Recourses	books, films, and interactive app and games	lesson, films, and games	books, films, and interactive app and games	Advice and videos
Audience	for young people, parents and teachers	for young people, parents, and teachers	for young people, parents and teachers	parents and carers
Age groups	primary and secondary students	different age groups (5-7, 8-10, 11-13, and 14+)	different age groups (3-11, 11-19)	different age groups (0-5, 6-10, 11-13, and 14+)
Website	http://www.childnet.com/resources	https://www.thinkuknow.co.uk/	http://www.saferInternet.org.uk	https://www.internetmatters.org/

3.3 Conclusion

This chapter has shown that existing parental control methods help parents to monitor and restrict children's Internet use, but do not assess the risk of children online activities and raise awareness about the potential risks that could help parents to make the right decisions. Also, there are some awareness initiatives present advice and different resources for raising awareness about Internet safety in separate websites. However, parents and children need to be aware of the potential risks and the implications related to their online activities in real time and means of safeguarding against them. Thus, Internet safety awareness initiatives should be integrated with parental controls. Risk awareness should form part of any parental control solution and can play an important role in children's safe use of the Internet.

Therefore, parental controls should help parents to know what their children do online and the associated risks, and thus they can identify the level of control suitable for their children's needs. To this end, risk communication technology could be used to predict and assess risks associated with children's online activities and raise awareness about the potential risks and help to make good security decisions. Risk communication technologies could help parents and young people understand the potential risks to which children may be exposed before the danger is actually realised. Thus, the next chapter considers and reviews risk models and communication.

Chapter 4: Risk communication framework for parental control

The Internet offers a very long list of services and opportunities, but also presents numerous risks. Unfortunately, most users are unaware of the implications associated with their online activities and most threats. Thus, users need to be aware of the potential risks. Risk communication is used as a first step in raising awareness and enabling people to make safe decisions. It is an interactive process of exchanging information regarding risk and includes the nature of risk, its meaning, consequences, likelihood and recommended options (Nurse, 2013). The following section presents a review of risk assessment and communication approaches employed to promote Internet safety. Then, a risk communication framework for managing children's Internet use is presented. Also, the proposed risk assessment model for calculating the risk level of children's online activities is presented. The last section presents protection response strategies. In addition, some scenarios of potential children's online behaviour are assumed and simulated in order to show how the proposed system could work in different situations.

4.1 Risk assessment and communication approaches to promoting online safety about specific security issues

The growth of digital technologies presents many new security threats to users. As these threats are quite difficult to handle, there is a need to make users aware of the potential risks they may face when they go online. Risk communication, therefore, is used to raise awareness about different security issues of users and helping them to make more conscious decisions.

Research has used risk communication to raise awareness about specific security issues such as malicious applications that invade privacy and collect and send a user's personal information to unauthorised third parties. Kang et al. (2015) proposed Privacy Meter, which evaluates the risks of application based on the application's permission requests, and visualises the computed

risk scores when user try to install the application. This enables users to recognise dangerous applications quickly and easily, and help to make privacy-conscious decisions.

Theoharidou et al. (2012) also proposed a method to assess the different risks associated with different mobile applications. The risk is assessed as a combination of asset impact that assessed by user and threat likelihood (the likelihood of permission combination acceptance and the statistics on threat incidents in platform). Risk was calculated on the basis of a risk matrix, and mapped as Low (0-2), Medium (3-5), or High (6-8), as shown in Figure 25.

Threat likelihood		Low			Medium			High	
Permission likelihood	L	M	H	L	M	H	L	M	H
	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
Asset impact	**2**	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

(Theoharidou et al. 2012)

Figure 25: Risk matrix for smartphones

Also, some risk communication models are emphasised on users' behavioural aspects such as sharing personal information on social media that may cause substantial risks, such as stalking, identity theft, damaged reputations, or loss of a relationship or job. Wang et al. (2013) designed a system that alert user to consider the content of their online disclosures more carefully before posting them on Facebook.

Kongkarn and Sukree (2012) also used risk communication to help parents to recognize their children's behaviours in online gaming. They proposed a model that tracks the child's interaction during the gaming (the type of gaming, and the duration and frequency of play), and then diagnoses the risk level of online gaming addiction and generates report about the risk level and suggests advice to parents.

Overall, several studies have used risk communication technology to inform users of specific online risks such as privacy invasion and Internet addiction. Also, most of current risk

communication approaches are aimed at promoting online safety for generic end users, whereas none of them focus on children's Internet use and promote online safety for young people and helping parents to control their children's Internet use. Users of different ages use the Internet for different purposes and encounter different risks with different impact consequences. Users also differ in terms of their cognitive abilities, attention, and memory. So, the main key to devising effective risk communication technologies is to deliver the right information to the right stakeholder in the right context at the right time. Thus, these risk communication approaches could be applied to child's Internet use context to assess the potential risks associated with children's online activities, and then raise awareness of potential risks for parents and children in a simple and understandable way and offer appropriate mitigating actions. So, the next section presents a risk communication framework for managing the potential risks of children's Internet use.

4.2 Framework for applying risk communication in parental controls

The existing parental control methods help parents to monitor and restrict children's Internet use, but also do not assess the risk of children online activities and raise awareness about the potential risks for parents and children to help them to make the right decisions. Also, most of current risk communication approaches are aimed at raising awareness of online safety for generic end users, while parents and children need to be aware of the potential risks and the implications associated with children's online activities and means of safeguards. To this end, risk communication mechanism should be integrated with parental controls to assess the potential risk associated with children online activities and help parents and children to understand these risks and safeguards in a continuous manner. The main contribution of this research is that it aims to apply risk communication mechanisms to parental controls in order to raise security awareness of the potential risks for parents and children in real time, so that they will have an opportunity to understand a potential risk before the danger is realised. In this research, the proposed system monitors children's online activities, assess the risk level of each

action, warn parents and children, and provide appropriate mitigating actions according to the risk level involved. The system provides a flexible and adaptable parental control that engages parents in the risk assessment process and gives them a granular level of control over their children's online activities. The following scenario is an example of how the proposed system would work: when a child shares personal information on a social network, the proposed system computes the risk level of that activity. If the risk level is high, the system takes preconfigured (default) protection responses, such as to disallow the activity, sends an alert to warn parents of a risky action, and offers mitigating actions, such as to push advice to the child or block the application.

The proposed framework was designed based on gaming addiction assessment framework that consists of three parts: behaviour tracking that tracks actual player interaction; a diagnosis of the risk level of online gaming addiction; and reporting that reports the results of the risk and advice to the parent. The framework also consisted of two knowledge bases: a risk level standard and the player's knowledge base (Kongkarn and Sukree 2012). The components were altered to adapt the framework to the aims of the proposed system for monitoring children's Internet use and assessing the risk levels of children's online activities, as shown in Figure 26. This system is composed of three main parts: a children's applications usage monitor, a risk assessor, and a responder; as well as three knowledge-based parts: the child's knowledge base and a risk database (activity risk levels and impact consequences); and a response action database (protection responses for children's activities). The Application Usages Monitor is in the child's device to monitor his/her online activities and send the data to the server. The child's data are stored in the child's knowledge database. The Risk Assessor uses the child's data to compute the risk level of the child's activities using the risk database, and the Responder issues the protection responses based on the resulted risk level. Thus, the proposed system consists of two parts: on children's devices, this part monitors the child's usage; on parents' devices, this part enables parents to set up an account for each child and manage their children's activities.

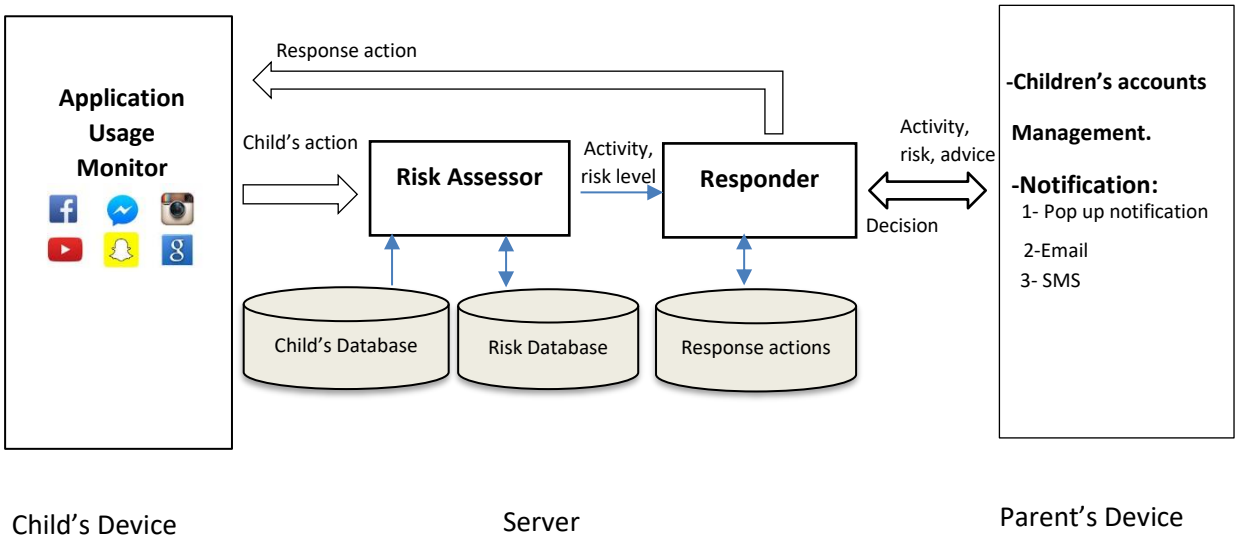


Figure 26: Risk communication framework for parents and children

As shown in Figure 25, the proposed framework consists of a number of key components: a children's activities monitor, a risk assessor, and a responder. These components perform various tasks, such as generating child profiles, calculating online risk, and sending notifications and advice.

- **Child's Application Usage Monitor:** This component aims to observe and monitor the child's activities. It collects variable data, including applications and actions, time spent (duration), frequency of use, and location, since these are necessary data in the process of calculating risk levels. The monitor part sends the child's data to the server, and the data are stored in the Child's Knowledge Database.
- **Risk Assessor:** The main function of the Risk Assessor is to calculate the risk of each action based on the proposed method, which is fetched from the Risk Database using information from the child's knowledge base. An action with a risk level value is forwarded to the Responder. In this context, the resulted risk level is given one of the following values: no risk, low, medium, or high.
- **Responder:** The inputs for this component are the action and the calculated risk level. Based on the risk level, the Responder makes an action taken from the Response Action

Database. This component can take action, such as disallowing an action and providing parents with information about the action and the resulted risk level, as well as security advice and additional mitigating actions. Mitigating actions include pushing advice to the child according to his/her age or limiting the time spent on that application.

4.2.1 Risk assessment model for children's Internet use

All children who access the Internet are potentially at risk of harm, but some children appear to be more likely to encounter risk and harm online. Thus, risk value is computed based on likelihood and impact (severity of harm). The likelihood is evaluated based on children online activities and individual factors of children that could raise the probability of harm to children. Thus, the following sections present young people's risky online activities and individual factors of child and his/her Internet use that could increase the probability of risk occurrence.

4.2.1.1 Young people's online activities

Some children's online activities are considered normal and are common when young people are using the Internet such as browsing websites, playing games, watching video clips and using social networks and communication platforms (Livingstone et al. 2019). However, there are some activities that could expose a child to online risks and harm as a result. For example, browsing websites could cause exposure to content risks, such as adult/abusive material, and commercial threats and spam. Children could search for an inappropriate content or receive pop-up windows. Also, children sometimes are manipulated to place unwanted orders or to visit unwanted commercial pages in a browser by having clicked on a page as a condition of accessing information (Magkos et al. 2014).

Using communication platforms could cause some contact risks, such as cyberbullying, grooming, sexting or privacy invasion, and Internet- related risks such as viruses, malware, and phishing. Some children engage in risky online behaviours in social networks such as making

new friends online with whom they have had no prior offline contact and communicating with them, exchanging images and meeting offline, or disclosing too much information about their personal lives.

Playing games also could expose children to content risks, such as inappropriate content and commercial threats, and contact risks such as cyberbullying. Young people might play games that are rated for much older children or games that have inappropriate content. Also, online game players might chat throughout a game to players they do not know, and there is a possibility of their being bullied by other players. In addition, some games collect and leak personal information, they ask a child to fill out lots of details before he/she can play and then illegally sell those data on to others (NSPCC n.d.). In addition, some games ask children to make in-game purchases in order to acquire additional points or tokens, levels, or game upgrades (Ofcom 2016).

Use of file-sharing platforms could expose children to content and contact risks such as inappropriate material or privacy invasion. Some children might search for pornographic or violent videos that might lead or tempt the child into unlawful or dangerous behaviour. Some children share videos that contain personal information, such as showing the front of the child's house or details of the home address, or about their school, for example by showing the school uniform. These types of video expose children to risks such as kidnapping and rape (Priestlands School, 2016).

Prior research also has summarized the high-risk behaviour, for example, DeMarco et al. (2017) identified the risky online activities that include giving out personal information online, downloading pirated material, accepting people as friends online without knowing them offline, visiting pornographic websites, sharing personal photographs or videos with strangers, and meeting people face to face that they have only met online. An Ofcom report has also referred to potentially risky online activities among children, which included the following: adding people to a friends or contacts list whom the child has only had contact with online; sending

personal information such as full name, address or phone number, or a photo or video of him/herself to a person only known online; and share location with other users (Ofcom 2016). Other research found that social network users encountered more risks than non-users, especially if they engaged in risky activities such as having a public profile that displayed personal information (Staksrud et al. 2013). Information that is considered personal under COPPA includes: full name, home or other physical address, online contact information, such as an email address or telephone number, a persistent identifier that can be used to recognise a user over time, including an IP address or device serial number, a photo, video, or audio file containing a child's image or voice, and geolocation information that identifies a street name and city ("Children's Online Privacy Protection Rule" 2013). Research found also that excessive Internet use, for example, using the Internet every day for more than two hours a day, could cause Internet addiction (Koyuncu et al. 2014).

Overall, children's activities have different risk levels, depending on the actions' participation in the occurrence of the online risks (content risk, conduct risk, contact risk, and computer/ Internet risks). Thus, Children's online activities can be categorised into four levels: no risk, low risk (activities that might lead to risk occurrence), moderate risk (indirect threats from participating to a degree in risk occurrence), or high risk (direct threats that result from direct participation in risk occurrence). For example, making new friends online with whom they have had no prior offline contact could be an indirect threat. In comparison, people who are unknown to them might communicating with children and gain their trust, with the goal of sexually abusing them during an offline meeting. Thus, arranging a time to meet an unknown individual offline could be considered a high-risk activity (direct threat), increasing the probability of risk occurrence and putting the child at risk of harm. The above-mentioned risky online behaviours pose a risk and can create different risk levels and concerns regarding a child's safety.

In the prototype presented in this research, the risk levels of most common risky online activities are initially assigned a descriptive value, which can be refined over time when using the system

in practice. The most common risky online activities and the potential risks are summarised in Table 4. The activity risk level could vary depending on parents' views and concerns. Parents would be able to assess whether or not an activity could expose their child(ren) to risk.

Table 4: *Risk levels of online activities*

Online activities		**Direct/ Indirect threat**	**Risks**				**Action contribution level of occurrence of risk (MAX)**
			Content risk (inappropriate content)	**Contact risk (sexual risk, sexting, psycho-logical risk, or privacy risk)**	**Conduct risk (illegal file sharing, unwelcome conduct)**	**Computer/ Internet-related risk, Internet addiction**	
Content related activities	Accessing / Searching for inappropriate content	Direct	3			2	3 (H)
	Downloading age-inappropriate applications	Direct	3	3	3	2	3 (H)
	Making a purchase	Indirect	2				2 (M)
Chat activities	Adding/accepting friend requests	Indirect		2	2	1	2 (M)
	Using a microphone/camera with unknown people	Direct		3	3		3 (H)
	Inappropriate chatting	Direct		3	3		3 (H)
Privacy-related activities	Sharing personal information	Direct		3	3	2	3 (H)
Time spent	Spending too much time with an application	Direct				3	3 (H)

4.2.1.2 Other factors that contribute to risk occurrence

There are some concern factors that raise the probability of harm to children. Previous research refers to different factors that affect young people's online experiences and exposure to online risk. In the system proposed in the research, the factors that influence young people's Internet experience and considered in the risk assessment process include child's age, the child's Internet access (locations and years online) and child's Internet use (frequency of Internet use and time spent online) (Livingstone and Helsper, 2010). Furthermore, there are other factors that could be added such as device type and psychological characteristics. If children have greater access, particularly via personalised and portable devices, they might encounter more risks (Mascheroni and Ólafsson 2014) (Stald et al. 2014). Also, children who had psychological difficulties report more online risks and more harm (Livingstone, Görzig, and Ólafsson 2011) (Vandoninck et al. 2013). There may also be other factors that could be added in future work.

Overall, these factors have an influence on the probability of exposure to online risks. Each factor have a different status based on numerical values (0: no effect, 1: least effect, 2: somewhat effect, 3: most effect). In addition, each factor can be assessed and given a weight value depending on its effect on the probability of the occurrence of online risks, as shown in Table 5. Each factor are given a descriptive value and weight in the proposed system. These numerical values could be refined and become more accurate after the practical use of the risk assessment model in a real environment and then considered in the system. Also, the practical use of the model might detect further factors that could contribute to the occurrence of risk and then could be considered in the system.

Table 5: Weight values of risk factors

Weight value	Explanation
1	The factor has a low effect and indirectly affects the probability of the occurrence of risks.
2	The factor has a slight/normal effect and somewhat affects the probability of the occurrence of risks.
3	The factor has a high effect and directly affects the probability of the occurrence of risk.

Individual factors of child

Some children might be more vulnerable to online risks than others due to individual factors that include child's age, psychological characteristics, and Internet experience.

1) Child's age

Age has an influence on online opportunities, Livingstone and Helsper (2010) find that age has a direct and positive influence on access and use, older teenagers have a better quality of access and use the Internet longer and thus encounter more online risks. Older children are more likely to use the Internet with more diverse use for more hours per day and with more technologies in more places. Thus, online risks are raised among older children who use the Internet more (Stald et al. 2014). Also, more than half of older children see the Internet as a way of 'being oneself' or talking about sensitive matters through online communication, and older children also encounter more online risks (Smahel et al. 2020).

As indicated above, a child's age could affect indirectly the probability of exposure to online risks. Older children have better access and had use the Internet longer and participate in a wide spectrum of online activities, and thus might encounter more online risks. Thus, age could somewhat affect the probability of the occurrence of risk and take a weighting of '2'in the proposed system. Thus, children and young people tend to be grouped into different age groups in which children have similar attitudes and behaviour (Ofcom 2016). The first group refers to children aged 4-7, the second group to those aged 8-11, and the third group

to those aged 12-16. Older children might encounter more risks because they have more access and participate in a greater number of online activities, and they are more adventurous and less obedient; and thus take the value 3. As young children usually have less access and limited activities and limited critical and social skills, they take the value 2, as shown in Table 6.

Table 6: Descriptive values for the age factor

Age	**Value**
4-7	2
8-11	3
12-16	3

2) Psychological characteristics (psychological difficulties, sensation-seeking)

There is also a range of adverse emotional and psychosocial characteristics that make some children more vulnerable to exposure to risk and harm than others, that include sensation-seeking, and psychological difficulties. Psychological difficulties may lead to higher risk-taking behaviour in the online context. Children who face psychological difficulties or tend towards sensation-seeking take more risks both offline and online (Livingstone and Smith 2014). Children with greater psychological difficulties (emotional, peer, or conduct problems) are more vulnerable and have a higher intensity of feeling upset (Vandoninck et al. 2013).

Children's psychological characteristics could affect directly children's behaviour and the probability of their exposure to risk. As children with psychological difficulties or who have a tendency to sensation-seeking take more risks offline and online, this factor directly affects the probability of the occurrence of risk and takes a weight of 3 in the proposed system.

Psychological difficulties could be measured by using the Strengths and Difficulties Questionnaire (SDQ) that contains acceptable psychometric properties for measuring a child's psychological difficulties. The SDQ includes items that are divided into scales: hyperactivity scale, emotional symptoms scale, conduct problem scale, and peer problem scale, as displayed

in Table 7 (Goodman et al. 1998) (Livingstone et al. 2011b). Each item is scored as follows: 0 = not true, 1 = somewhat true, and 2 = certainly true. The resulting total score ranges from 0 to 40 and the child can be classified depending on the initial bandings provided for the SDQ scores: 0-13 = 'normal', 14-16 = 'borderline', and 17-40 = 'abnormal'. Sensation-seeking is measured using a shorter two-item measure that focuses on the risk-taking elements of sensation-seeking, which is very good overall as a measure for predicting risk. The response is measured using the following scale: 0 = not true, 1 = somewhat true, and 2 = certainly true (Stephenson et al. 2003) (Livingstone et al. 2011b), as shown in Table 8. The resulting score ranges from 0 to 4, and the child's sensation-seeking can be measured using a four-point scale: 0 = not sensation seeker, 1 = low sensation seeker, 2 and 3 = moderate sensation seeker, and 4 = high sensation seeker. These measures could be used to help parents assess their child(ren)'s psychological difficulties and degree of sensation-seeking.

Table 7: SDQ for children aged 4-17 (Goodman, Meltzer, and Bailey 1998)

Item	**Item description**
Emotional problems	
1	Often complains of headaches… (I get a lot of headaches…)
2	Many worries… (I worry a lot)
3	Often unhappy, downhearted… (I am often unhappy….)
4	Nervous or clingy in new situations… (I am nervous in new situations…)
5	Many fears, easily scared (I have many fears…)
Conduct problems	
6	Often has temper tantrums or hot tempers (I get very angry)
7	Generally obedient… (I usually do as I am told)
8	Often fights with other children… (I fight a lot)
9	Often lies or cheats (I am often accused of lying or cheating)
10	Steals from home, school or elsewhere (I take things that are not mine)
Hyperactivity	
11	Restless, overactive… (I am restless…)
12	Constantly fidgeting or squirming (I am constantly fidgeting….)
13	Easily distracted, concentration wanders (I am easily distracted)

14	Thinks things out before acting (I think before I do things)
15	Sees tasks through to the end… (I finish the work I am doing)
Peer problems	
16	Rather solitary, tends to play alone (I am usually on my own)
17	Has at least one good friend (I have one goof friend or more)
18	Generally liked by other children (Other people my age generally like me)
19	Picked on or bullied by other children… (Other children or young people pick on me)
20	Gets on better with adults than with other children (I get on better with adults than with people my age)

Table 8: Sensation-seeking measure (Stephenson et al. 2003)

Item	**Item description**
1	I do dangerous things for fun
2	I do exciting things, even if they are dangerous

3) Child's experience

Children who access the Internet earlier might learn skills from an early age and might also encounter risks earlier (Livingstone, Haddon, et al. 2014). Young people might acquire digital literacy by engaging with online and mobile platforms, according to EU Kids report the level of digital skills for older children is higher than that for younger children (Livingstone, Haddon, et al. 2014) (Smahel et al. 2020). Older children more widely appreciated safety skills than younger children. Children's awareness and understanding of potential online risks appears to increase with age, primarily due to education at school, increasingly diverse use of the Internet, as well as learning from friends and family members (Ofcom 2014b). However, digital skills might not reduce the likelihood that children exposure to online skills (Staksrud, Ólafsson, and Livingstone 2013a). Furthermore, some children are confident online in terms of their knowledge and skills but intentionally or unintentionally engage in risky online behaviour without understanding the consequences (Scott 2016).

Thus, children's Internet experiences and skills acquired from these experiences might be insufficient and do not reduce the likelihood of risk incidents. Therefore, Internet experience

might be the least effective factor in the probability of exposure to online risk, and thus takes a weight of 1 in the proposed system. There are four levels of Internet experience: novice (up to 1 year of experience), intermediate (2 to 3 years of experience), and advanced (more than 3 years of experience). Children of different ages could also have different skills, even if they have spent the same number of years online. Based on children's awareness and understanding of potential online risks appearing to increase with age, Internet experience is here calculated based on two factors: age and years online. A child's experience value is calculated according to the age class: years online and values for each age band (children aged 12-16 are represented by the value 1, children aged 8-11 are represented by the value 2, and children aged 4-7 are represented by the highest value of 3 because young children have a limited understanding and activities even if they use the Internet at an earlier age), as shown in Table 9.

Table 9: Internet experience results for children in different age groups

Years online categories	**Years online default values**	**Age groups**		
		Children aged 12-16 (years online +1)	**Children aged 8-11 (years online +2)**	**Children aged 4-7 (years online +3)**
Novice (up to 1 year)	3	4	5	6
Intermediate (2 to 3 years)	2	3	4	5
Advanced (more than 3 years)	1	2	3	4

Experience results are assigned according to the following scale: 0-2 = low, 3-4 = medium, and 5-6 = high. Internet experience values based on years online and the child's age are shown in Table 10.

Table 10: Internet experience factor values

Internet experience value	**Age groups**		
	Children aged 12-16	**Children aged 8-11**	**Children aged 4-7**
No experience	3	3	3
Novice (up to 1 year)	2	3	3
Intermediate (2 to 3 years)	2	2	3
Advanced (more than 3 years)	1	2	2

Factors related to children's Internet access

Internet access was measured in two ways: locations used to access the Internet and type of device used to access the Internet. Young people with more access locations benefit from other facilities associated with that access (e.g., more independent, and unsupervised access) and might, as a result, encounter more risks. Livingstone and Helsper (2010) found that the number of access locations has a significant direct influence on online opportunities and risks.

Also, better-quality access (e.g., fast connectivity and more powerful machine) through mobile devices facilitates more use and greater risk. Also, mobile devices provide anytime, anywhere accessibility. On the other hand, mobile media has increase online risks and introduced new risks, such as geolocation data and apps that connect children with strangers. Geopositioning services offer significant opportunity for the abuse of personal data, geolocation tracking, and threats to privacy for the purpose of commercial goals or grooming (Stald et al. 2014). Thus, Net Children Go Mobile report finds that the use of smartphone and tablet is linked to a rise in the number and types of online risks (Mascheroni and Ólafsson 2014). Thus, the child's Internet access (device type and locations) is the most important factor and has a positive and direct influence on online risk. Therefore, this research proposes that these factors have the highest weight value: 3.

1) Location

Children access and use the Internet in different places, they can use the Internet in their bedroom, home or any other place. Thus, a wider range of access locations leads to more unsupervised access and more independent Internet use, that involve more opportunities and risks (Livingstone and Helsper 2010). Each location of use implies different levels of freedom, privacy, sociality and surveillance. When children use the Internet in private places, they could escape their parents' supervision. In addition, young people often feel safer doing risky activities online such as sharing sensitive personal information or engaging in sexualized behaviour, than they do offline, furthermore, children engaged in online activities such as chat online in the private place (i.e., bedrooms) can expose themselves wittingly or unwittingly to risky online behaviour (UNICEF Innocenti Research Centre 2011).

The EU Kids Online survey found that approximately half (49%) of all children who used the Internet did so in their bedroom or another private room at home, and 62% used it in the living room or other public room at home that could be monitored by parents (Livingstone et al. 2011a). In 2019, Ofcom report finds that most of parents allow their children to go to bed with their mobile (63%) (Ofcom 2019b). Children also access the Internet in school, which can be monitored by teachers. Schools are generally highly supervised locations of use.

Thus, the model proposed in the present research will assign a score to each place used to access the Internet (e.g., bedroom or private room, other public rooms at home, school, or other places) based on the effect of increasing the probability of exposure to online risk, as shown in Table 11. As it is difficult for parents to share or observe their child(ren)'s Internet use in private rooms, children may enjoy unsupervised access in these private locations and take up more opportunities and more risks, and therefore a value of 3 is assigned to private locations as this increases the probability of exposure to risk. In comparison, children might feel restricted in public rooms in the home as they might be observed by parents or other family members, and thus take a value of 1. Also, schools might be supervised by teachers and thus take a value of

1, whereas other places, such as parks or cafes, where children are unobserved, are given a value of 2.

Table 11: Descriptive values for the location factor

Location	Value
Private rooms, e.g., bedroom	3
Public rooms in the home	1
School	1
Other places	2

2) Device type

Mobile media has expanded Internet use and communicative practices among children by providing 'anywhere, anytime' accessibility, which causes difficulties for parents in supervising their children's behaviour. The speed and ease of mobile access have also increased the risks encountered by children. Children could act without thinking about the possible negative consequences of their actions, they can immediately distribute and share user-generated content such as that related to sexting or cyberbullying through a mobile device. Furthermore, mobile media has introduced new risks, such as geopositioning services that can locate a mobile user's position and connect that user with services and people (Stald et al. 2014). Thus, previous studies have found that children with access to a smartphone or tablet were more likely to have encountered one or more online risks. The Net Children Go Mobile data study (2013) and EU Kids Online (2010) found that there was a significant difference in risk exposure between children who did not use a mobile device and those who did. The EU Kids Online study found that 10% of children who did not use mobile devices encountered three or more risks, while 19% of children who used such devices encountered three or more risks. Net Children Go Mobile found that 37% of children who used mobile devices encountered one or two risks and 20% encountered three or more risks, whereas 26% of children who did not use mobile devices encountered one or two risks and 8% encountered three or more risks. The risks encountered were greater in the group of children with mobile devices than in the group without,

as mobile devices enable children to access the Internet anywhere and at any time (Stald et al. 2014) (Staksrud, Ólafsson, and Livingstone 2013b). In addition, some parents seem to have trusted their children who had mobile devices to make good choices, and were less likely to lay down rules around their child's Internet activities (Stald et al. 2014).

Therefore, device type has an important effect on the probability of exposure to online risk. In the proposed prototype, each device (mobile phone, laptop, or desktop) used to access the Internet has a different value, which depends on its impact on the probability of exposure to online risk. Descriptive values were assigned to each device based on the previous discussion, as shown in Table 12. The speed and ease of mobile access encourage children to behave immediately without thinking about the possible negative consequences, and make supervising children's mobile use is difficult for parents, so, mobile devices have the highest value: 3. Children's use of fixed computers, such as desktop computers, puts them at a lower level of exposure to risk than mobile devices, and thus desktop computers take a value of 1.

Table 12: Descriptive values for the device type factor

Device type	**Value**
Desktop	1
Laptop	2
Mobile device	3

Factors related to children's Internet use

This factor was measured in two ways: frequency of Internet use and time spent online. Children's who use the Internet more, they take up more opportunities and they might encounter more risks. According to Livingstone et al. (2011a), "children's experiences of online opportunities and risks go hand in hand – the more of one tends to mean the more of the other". Livingstone and Helsper (2010) find that the time spent online has a significant direct influence on online opportunities and risks. Also, Ofcom study show that children's exposure to online risks increase with increased time spent online especially in weekend (Ofcom 2020). So, the time spent online could directly affect the probability of exposure to online risks, and thus take

a weight of '3'. Frequency of use could increase the opportunities taken up, so, it could somewhat affect the probability of the occurrence of risk and take a weighting of '2'in the proposed system.

1) Frequency of use

More Internet use by children might expose them to online risks. More frequent use by young people encourage them to take up more online opportunities and do more on the internet, and this might result in more risk (Livingstone and Helsper 2010a). Prior research has observed young people use of applications. Some research found that children visited their main social media application every day. For example, a study conducted among 13 to 17 year olds found that approximately half (51%) of them checked their social networking sites daily (A Common Sense Media Research Study 2012). Other research found the average daily use of games to be three times a day (Brand and Todhunter 2016) and the average use of social network one to five times a day (Kirik et al. 2015).

More frequent daily use of Internet is associated with more opportunities and probability of exposure to online risk. Thus, the frequency of Internet usage is measured in the proposed system on the basis of the following options: once a month or less than once a month, once or twice a week, 1 to 5 times a day, or more than 5 times a day, as shown in Table 13.

Table 13: Descriptive values for the frequency factor

Frequency of use	**Value**
Once a month or less	1
Once or twice a week	1
1-5 times a day	2
More than 5 times a day	3

2) Duration (time spent)

Excessive use of the Internet by children expose them to more online risks (Ofcom 2020). Prior research has measured the amount of time young people spend with media. For example, the overall time spent online by children was found to be around one-and-a-half hours per day (88

minutes) (Livingstone et al. 2011b). Common Sense research conducted a study of media use with a sample of 2,658 young people aged 8-18 and documented the amount of time young people spent in different media activities, as shown in Table 14 (Rideout 2016). Also, the DinnerTime Plus application released statistics on the average time young people spent on different applications, as shown in Table 15. The sample contained more than 2,800 children and showed that the average daily application usage was 183 minutes (3 hours and 3 minutes), with communication applications such as Instagram and Facebook the most popular applications used among young people ("Kids Spend More Than 3 Hours a Day on Apps" 2014). In addition, the American Academy of Paediatrics recommends limiting a child's viewing of movies, watching TV, and playing video games to one or two hours per day. Booker conducted a study about the lifestyles and emotional well-being of around 5,000 young people aged 10-15 and found that more than half of UK young people used social networks such as Facebook, Twitter and Snapchat for at least one hour every day (Booker 2014). Also, another study used two hours per day as moderate SNS use and heavier SNS use as more than two hours daily) (Tsitsika et al. 2014).

Table 14: Average time per day spent with different applications by US youth, 2015 (Rideout, 2016)

Applications	**Among 8-12 year olds**	**Among 13-18 year olds**
Playing games	1:19	1:21
Using social media	0:16	1:11
Browsing websites	0:12	0.36

Table 15: *Average time young people spent with different applications per day* ('Kids Spend More Than 3 Hours a Day on Apps', 2014)

Applications	**Duration (minutes every day)**
Social/messaging applications	65
Games such as Minecraft - Pocket Edition and Clash of Clans	52
Video-sharing platforms, such as YouTube and Netflix	86
Internet browser, such as Google Chrome	22

Therefore, as length of time online contributes to the probability of exposure to online risk, time spent online will be measured in the proposed prototype based on the following options: about half an hour, about one hour, between one and two hours, or more than two hours. Default values for each application category are assigned based on the previous studies that present the average time spent in different applications, and are shown in Table 16.

Table 16: *Descriptive values for the duration factor*

Duration	**Games**		**Social networks**		**Web**		**Video-sharing platforms**		**Overall time spent**
	4-12 years old	**13-16 years old**	**4-12 years old**	**13-16 years old**	**4-12 years old**	**13-16 years old**	**4-12 years old**	**13-16 years old**	**4-16 years old**
Half an hour	1	1	1	1	1	1	1	1	1
1 hour	1	1	2	1	2	1	1	1	1
1-2 hours	2	2	3	2	3	2	2	2	2
More than 2 hours	3	3	3	3	3	3	3	3	3

4.2.1.3 Impact assessment

Assessments of impacts related to children's Internet use (online activities) focus on the harm caused to children and parents. Different activities can lead to different consequences, including those linked to the following: child safety, social harm (e.g., loss of friends, being ostracised), invasion of privacy, disruption, and financial loss (Magkos et al. 2014) (Livingstone 2013).

Impact on personal safety

Child safety can be threatened by physical harm, such as injury or bodily attack, emotional harm, such as feeling upset or threatened, and psychological harm, such as low self-esteem and the consequences of violence (Magkos et al. 2014) (Livingstone 2013). Different online activities might expose children to online risks that affect their safety in various ways. Communicating with unknown people or sharing personal information on social networks could

affect child's safety and expose them to cyberbullying, sexual exploitation and rape or kidnapping (Fire, Goldschmidt, and Elovici 2014) (Santisarun and Boonkrong 2015). Also, accessing inappropriate content might upset young people or promote eating disorders, self-harming behaviour, drug consumption, discrimination, or violence (Livingstone, Haddon, Vincent, Mascheroni, and Ólafsson 2014). Furthermore, some games contain violence that make them violent and engage in anti-social behaviours. Violent and bullying behaviour in the online world can have a significant effect in the physical world (traditional bullying). Young people who had experienced repeated cyberbullying instances in online gaming were found to have had a greater likelihood of observable aggressive behaviour in daily life (Fryling et al. 2015) (Shu Ching Yang 2012). Thus, children's access to inappropriate content might draw them into doing things they would never do offline because the behaviour of other users makes it appears right (NSPCC n.d.). Also, spending too much time on the Internet might have other negative effects, such as an increased possibility of developing depression, anxiety, attention problems, isolation, weight gain or loss, and blurred or strained vision ("Signs and Symptoms of Internet or Computer Addiction" n.d.).

Social harm

Children's social relationships also could be affected by their Internet use. Children can use communication platforms and contact unknown people, which might lead to receiving hurtful or sexual messages or the publishing of embarrassing pictures or videos of children. Cyberbullying takes place and has become common on SNSs, children were cyberbullied and cruel rumours about them are spread and they were upset and losing friends (Fire et al. 2014) (Livingstone et al. 2014). Some online games also enable players to connect with each other, creating the possibility of players sending harassing messages to their opponents. Bullying among players can take the form of sending obscene or violent threats that have the aim of gaining power or control over other players (Sandhu 2015). Thus, bad use of the Internet has an impact on the social relationships between children.

Impact on personal privacy

Children's Internet use can cause serious invasions of their privacy. Children who are unaware of the risks related to the inappropriate use of their personal information often participate in privacy leakage (Jeong and Coyle 2014). The disclosure of children's personal information in a social network profile exposes children to information theft, tracking, and phishing (Santisarun and Boonkrong 2015). In addition, advertisers and marketers could use children's information to craft personalised messages for them (Jeong and Coyle 2014) (Santisarun and Boonkrong 2015). There are also games that collect children's information and sell those data illegally to others (NSPCC n.d.).

Financial loss

Children's Internet use could cause financial loss. For example, children might be duped by advertisements that offer prizes, such as "you've won an iPod". After the child enters his/her phone number, he/she is then charged money (Haddon and Vincent 2014). Furthermore, some games include in-app purchases hidden behind a free download. These games offer a small amount of play and then charge for continued use, offering in-app purchases for extra areas of play or upgrades. Children can also download games that charge money for every SMS they send (Haddon and Vincent 2014), thereby causing considerable financial loss.

Impact of disruption

Some circumstances or events can interrupt and disrupt services and the functions of applications. Some applications, games, and files contain viruses that disrupt device services when they are downloaded. Attackers are also able to hack SNS profiles by using malicious codes or social engineering. They can then, for example, access a child's profile and change the passwords (Livingstone, Haddon, Vincent, Mascheroni, and Ólafsson 2014). Phishing is another of the common means of tricking children into revealing private information after receiving an email to a fraudulent link (Sharma n.d.).

Online risk varies in terms of severity (from high to low). The impact values of each activity are different. For example, accepting unknown people's activity or sharing personal information could affect a child's privacy, while inappropriate chatting activity could have a strongly negative effect on a child's safety. Thus, each risky activity can be evaluated in terms of potential consequences, the proposed system using a scale from 0 to 3 (0 = no impact, 1 = low impact, 2 = medium impact, and 3 = high impact), and the impact value for each activity is then the maximum value of the consequences. The impact types could be different according to parents' personal views (i.e., whether or not someone initially thought that there was a problem that bothered them).

4.2.1.4 Risk calculation

In the proposed system, the overall risk value is calculated based on impact consequence and likelihood. To assess the level of the potential impact of each activity, the "worst-case scenario" principle is used and the maximum impact value is used.

There are different ways to compute the likelihood of exposure to online risk. The likelihood of risk occurrence could be calculated based on the individual factors of child and behavioural factors (online activities). Behavioural factors could be more important than individual factors of child, especially when parents are concerned about specific activities and need to manage those activities. Risky behaviour could affect and contribute directly to a child's exposure to online risks, whereas individual factors of child could somewhat increase the probability of exposure. In this case, the likelihood is computed using a risk matrix for each risk behaviour level: low risk action, moderate risk action, or high risk action. This way of computing the likelihood of risk occurrence is proposed as a basis for the prototype system. In addition, if parents have different concerns regarding their children, the system prototype enables them to manage each child individually in relation to assessing the child's activities and determining appropriate responses. The likelihood of experiencing online risks is calculated using the following formula, and likelihood results are presented in Table 17. The likelihood value could

be categorized into five levels: Very Low (0-10), Low (11-20), Medium (21-30), High (31-40), or Very High (41-51).

$$\sum_{n=1}^{6} W_i P_i$$ (Karabacak and Sogukpinar 2005)

Where,

i = the number of factors, W = the weight of the factor, P = the value of the selected option of the factor

Likelihood = Age * W(A) + Psychological Difficulties * W(PD) + Sensation-Seeking * W(SS) +

Internet Experience * W(IE) + Location * W(L) + Device Type * W(DT) +

Duration * W(D) + Frequency * W(F)

Table 17: Probability values

Probability result	**Qualitative scale**	**Quantitative scale**
0-10	Very Low	1
11-20	Low	2
21-30	Medium	3
31-40	High	4
41-51	Very High	5

The risk value for each action is calculated by multiplying the impact by the likelihood, risk can be mapped as Low (1-5), Medium risk (6-10), or High risk (≥11). Thus, the risk value is exacerbated with increase of the likelihood (activity risk level and individual factors of child), as shown in Table 18.

Table 18: Risk matrix for different risky activities

	Likelihood														
	Action risk level	**Low**					**Medium**					**High**				
	Child's individual factors	**VL 1**	**L 2**	**M 3**	**H 4**	**VH 5**	**VL 2**	**L 3**	**M 4**	**H 5**	**VH 6**	**VL 3**	**L 4**	**M 5**	**H 6**	**VH 7**
Impact	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	2	3	4	5	2	3	4	5	6	3	4	5	6	7
	2	2	4	6	8	10	4	6	8	10	12	6	8	10	12	14
	3	3	6	9	12	15	6	9	12	15	18	9	12	15	18	21

4.2.2 Protection responses

There are some common protection responses that can be given to the various risk levels that result from different online activities, such as blocking, alerting and reporting to the parents, limiting the time for using an app, raising the awareness of the child, and enabling communication between the child and his/her parents.

Blocking response

The blocking response (stopping power response) offers different choices, such as termination of a specific process or session and blocking an application, Internet use, or device. These responses have different disruption levels in relation to a child's use of applications.

Alerting and reporting to parents

This type of system enables parents to receive an alert immediately their child's activities present a risk. The alert informs parents of the risky activity and gives them additional protection responses. Parents can also receive a report of their child's online activities on different applications.

Limiting time response

Parents can set time limits on individual applications. They could also select a specific period of the day or week for using those applications (e.g., allowing access for one hour every day). In addition, parents can restrict a child's use of an application to a specific time of day (e.g., allowing access from 7 am to 6 pm every day).

Raising the awareness of the child

Awareness raising and advice can differ according to the risk type and the child's role. A child plays different roles: he/she could be a recipient of risks, or a participant in the occurrence of risks. When a child receives an online threat, he/she could be targeted by the threat (target recipient) or not targeted (non-target recipient). For example, a child could be a target recipient of threat and receive a sexual message, whereas a child could be a non-target recipient of threat when receiving inappropriate or adult pop-up windows. Thus, when a child's role is that of receiver, the system will warn the child about the effect of exposure to inappropriate content and contact and advise him/her on how to deal with incidences of harmful and inappropriate content and contact.

A child might participate intentionally or accidentally in the occurrence of risks. For example, a child might accidentally access inappropriate content or intentionally contribute to risky content, such as by undertaking a search for violent or harmful content. Thus, when a child is a participant, the system response should be to protect the child by warning him/her of the consequences of that behaviour and advising him/her to reduce and stop harmful and inappropriate contact and conduct.

In addition, awareness-raising interfaces could be developed to be suitable for advising children at different ages and with different cognitive ability levels. Awareness raising could advise children on how to avoid online risk and measure their understanding and reaction to the advice. The system could also provide resources for more information and advice.

Enabling parents to communicate with their children

This type of system allows parents to contact their children and advise them and to do so through a text message, voice call, or video call. The system enables parents to contact their children and discuss their online activities because, according to previous research (Livingstone, Mascheroni, et al. 2014), most parents prefer to use active mediation. The proposed system can also advise parents and offer them resources to obtain more information and advice in order to have a sensible conversation with their children. Parents can then advise and explain to their children why some activities are inappropriate or dangerous and give them advice about how to use the Internet safely.

Response characteristics and selection

Protection responses have general characteristics, including response execution (automatically by the system or manually by the parent), response type (active responses that a child will notice, or passive responses that work in the background and the child is not aware of them), and impacts on the child (disruption level) as some responses might have a high effect on children, such as those that deny access to specific applications, whereas others might only moderately affect children, such as limiting the time for using an application or device. (Papadaki and Furnell 2006). The overall protection response phases and their characteristics are shown in Table 19.

Table 19: Protection responses and their main characteristics

Response	Response options	Response type		Response execution			Impact on a child
		Active	Passive	Automatic	Manual	Both	Disruption level
Blocking	Termination of process/session	✓				✓	3
	Block application	✓				✓	4
	Block Internet use	✓				✓	5
	Block device	✓				✓	6
Alert and report to parent	Send an alert to parents		✓	✓			0
Limiting time	Limit time for a specific app (hours-days)	✓				✓	2
	Limit time for Internet use (hours-days)	✓				✓	2
Raising awareness	Warn children of their behaviour (consequences) and instruct them in how to avoid it (text, image, or video)	✓				✓	1
Enabling parents to communicate with their children	Parents advise their children through a text message, voice call, or video call.	✓			✓		1

Different risk values (obtained by the multiplication of impact and likelihood) resulted from different online activities need different protection responses. Appropriate responses to different contexts can be selected according to risk level. The system assigns default protection responses for different risk levels. Parents are also able to customise and configure the process of response selection. Thus, the selection of appropriate response phases is mainly affected by the alert level (risk level). If the alert is high, the system performs an automatic stopping power response (i.e., blocking) to protect the child, and raises the child's awareness of the risk. The system also informs parents and gives them further options, such as additional blocking or communicating with their child to advise him/her. If the alarm level is medium, the child will be supported with low disruption responses, such as raising the child's awareness, and the system informs the parents and gives them further options, such as additional blocking or communicating with their child to advise him/her. If the alert level is low, no response will be taken and the child can be monitored and activities reported to the parents.

The efficiency of the responses in different contexts can be measured based on the effect of the response on protecting the child against a threat. The efficiency value for each response can be refined over time through the experience of the system, and efficient responses could be assigned to each activity for children in different age groups. Thus, the system would be able to recommend appropriate responses.

4.3 Simulation of system reaction with different scenarios

The system framework has been developed to be implemented within a real-world environment. However, implementing a fully functional system is difficult due to the research programme being limited by a certain time frame and the need for the system concept to be assessed with parents to ascertain that the system would be usable, acceptable and satisfactory. Therefore, a simulation approach was used to imagine the way in which the real system would work. Incidents from media reports were employed as factual accounts. The following sections

present different scenarios of contact and conduct risks, content risks, and computer/Internet risks; and demonstrate how the system could respond in different situations to protect children.

4.3.1 Scenario related to real-world stories of children's participation in interactive situations and exposure to contact and conduct risks

Contact and conduct risks can occur through social networks or chatting in games, children participate in an interactive situation and being victims (contact risk) or aggressor (conduct risk). Contact risks involve children being bullied, harassed or stalked. Media reports (the *BBC Magazine)* presented disturbing details about a story of a girl (aged 13) who was being harassed and kidnapped by a man (aged 38) after they had been chatting online. Her story was reported in her own words in the *BBC Magazine*:

> *At that time the Internet was really just entering the home. They had talked to me about "stranger danger" but there is a difference between a stranger you meet on the street and the stranger you meet online. People online may be strangers at first, but then you learn about them, and soon they seem like friends.*
>
> *I got online. My friends and I would talk about all sorts of things. There was one guy, a boy who I thought was around my own age, that I didn't know, and he was into all the things that I was into. He listened to what I had to say day and night, giving me advice. He was somebody to complain to and to get comforted by over the eight or nine months before my abduction. He was the one I walked out to see on New Year's Day and who kidnapped me in his car* ("Kidnapped by a Paedophile I Met Online" 2016).

Another story, reported in *The Independent* newspaper, involved the mother of a girl aged 11 talking about the bad experience that had happened to her daughter, who was receiving sexually abusive messages:

> *I didn't want my daughter to have Facebook: the legal age is 13 and she was still only 11. All the kids at school were talking about it; she said she felt left out. "Please mum please mum please mum." I set her account to private and told her explicitly that she wasn't allowed to make friends with anyone she didn't know.*
>
> *He managed to make "friends" with other girls at her school and by the time he came to request my daughter. The picture she saw on his profile was a blurred photo of a teenager wearing what looked like school uniform. He called himself Jack Smith. My daughter wasn't sure if she knew him, so she presumed that she did, and she accepted him.*

> *It began with him sending her friendly messages, a few jokes. This progressed to asking her to turn the webcam on. She resisted at first, but they were building up a friendship and in the end she felt obliged. She turned the webcam on but didn't show herself, instead she placed one of her teddies in front of the screen. He was on his webcam. He began sending her sexually abusive messages* (HANNAH 2017).

Also, conduct risks involve a child being involved in activities such as bullying or harassing other children, or creating and uploading inappropriate or harmful material. Abc news reports some incidents of children's sharing an inappropriate content, a 15- year old girl sent nude pictures of herself to classmates, and another boy also sent a sexual video of himself to classmates and one of them then forwarded the video to 30 other people. Young people don't understand the consequences of posting something online and how could become public very quickly, they also thought the fame can be had quickly by simply publishing a sexually explicit video on the Internet (GRANT 2008). Also, some children could bully and harass their peers at school, for example, a girl has taken photos of another girl and posted them on Snapchat calling her fat and ugly that affect badly the victim, and this led girl to feel isolated and have suicidal thoughts (Livingstone et al. 2017).

Generally, the children in the accounts above had engaged in risky behaviour. The resulted predicted risk from one action could be different depending on activity risk level (action's participation in the occurrence of online risks) and child's individual factors (age, experience, psychological characters, and child's Internet access and use). In the previous stories, children conducted different risky activities that include using social network application (Low risk activity), adding unknown people (Moderate risk activity), and an inappropriate chatting such as sharing personal information, or receiving/sending an inappropriate content (High risk activity). To calculate the risk value in the previous stories, two examples of children are considered to show the effect of the other factors on resulted risk value: the worst-case scenario (i.e., child is at a high risk level, who has a better access through using mobile device in private places and use the Internet for long time) and the best-case scenario (i.e., child is at low risk

level, who has a poor access through desktop device in public place and spend less time on the Internet). So, risk value is calculated using the default values.

Best case scenario (child is at low risk level)

Likelihood = 2×2 + 1×3 + 0×3 + 1×1 + 1×3 + 1×3 + 1×3 + 1×2= 19 = Low

Worst case scenario (child is at high risk level)

Likelihood = 3×2 + 0×3 + 3×3 + 3×1 + 3×3 + 3×3 + 3×3 + 3×2= 42 = Very High

If **activity risk level= Low and Impact = Low**
Likelihood= L --> R= L
Likelihood= VH --> R= L

If activity risk level= Medium and Impact= Medium
Likelihood= L --> R= M
Likelihood= VH --> R= H

If activity risk level= High and Impact = High
Likelihood= L --> R= H
Likelihood= VH --> R= H

So, if a child conduct low risk activity (e.g., using SNS activity), then the risk value is low in both scenarios. When a child is at low risk level and conduct moderate risk activity (adding unknown people), the risk value will be medium; while when conduct a high risk activity (an inappropriate chatting), the risk value will be high. On the other hand, when a child at a high risk level, the risk value will be increased significantly with different activities, for example, when a child conduct a moderate risk activity (adding unknown people), the risk value is raised and become high, and also when he/she conduct a high risk activity (an inappropriate chatting), the risk value is high. Overall, the risk values could be differ according to activity risk level and other factors related to child and his/her Internet use. So, the proposed system will monitor a child's activities, computer risk level, and take different actions at different stages depending on the resulted risk value in order to protect the child, as presented in Table 20. When the risk value is low, the system will monitor the child's activities in these apps, and report to parents.

If risk level is medium, the system will raise awareness for child about the danger of this action, and warn parents and give them some options for protecting their children such as blocking that use or enabling parents to contact their children by voice, text, or video call and advise them. If risk level is high, the system will terminate this action, warn a child, and inform parents and giving them other options: additional blocking, or communicating with their children.

Table 20: System's responses to different risky activities of chatting with strangers in social networks

Outputs			**Outputs**				**Result with system intervention**
Risky behaviours	**Risky activity level**	**Risk value = L×I**	**System intervention and response**	**Auto or manual**	**Active or passive**	**disruption**	
1. Using an inappropriate app (Kik, Yahoo).	L	R=L	Inform parents through report.	Automatic	Passive	0	Child is monitored
		R=M	1. System makes the child aware and advises about the danger of the app.	Automatic	Active	1	Child is warned.
			2. Informs parents and gives them additional protection options: • disallow the activity; • contact their children (voice, text, or video call) to advise them; • blocking (block app, Internet use, device); • limit time for using the app.	Automatic	Passive	0	Child will be advised by parent and/or restricted based on parent's decision.
		R=H	1.System terminates the process (using the app).	Automatic	Active	3	Child is restricted
			2.System makes the child aware and advises of the danger of using this application.	Automatic	Active	1	Child is advised.
			3. Informs parents and gives them additional protection options: • allow this activity; • contact their children (voice, text, or video call) to advise them; • blocking (block app, Internet use, device); limit time for using the app.	Automatic	Passive	0	Child will be advised by parent, and/or restricted based on parent's decision
2. Adding strangers	M	R=L	Inform parents through report.	Automatic	Passive	0	Child is monitored

		R=M	1. System makes the child aware and advises of the danger of strangers and how to deal with them.	Automatic	Active	1	Child is advised.
			2. Informs parents and gives them advice and additional protection options: • disallow the activity; • contact their children (voice, text, or video call) to advise them; • blocking (block app, Internet use, device); • limit time for using the app.	Automatic	Passive	0	Child will be advised by parent, and/or restricted based on parent's decision
		R=H	1. System terminates the process (adding the person).	Automatic	Active	3	Child is restricted
			2. System makes the child aware and advises of the danger of strangers and how to deal with them.	Automatic	Active	1	Child is advised.
			3. Informs parents and gives them additional protection options: • allow this activity; • contact their children (voice, text, or video call) to advise them; • blocking (block app, Internet use, device); • limit time for using the app.	Automatic	Passive	0	Child will be advised by parent, and/or restricted based on parent's decision
3. An inappropriate chat. • Receive a request for child's location or sexually abusive messages. • or send an inappropriate content (e.g., nude photo of themselves)	H	R=L	Inform parents through report.	Automatic	Passive	0	Child is monitored
		R=M	1. System makes the child aware and advises of the danger and consequences of this chat.	Automatic	Active	1	Child is warned.
			2. Inform parents and give them additional protection options: • disallow this activity; • conceal inappropriate chat; • contact their children (voice, text, or video call) to advise them;	Automatic	Passive	0	Child will be advised by parent, and/or restricted based on parent's decision

			• blocking (block person, app, Internet use, device); • limit time for using the app.				
		R=H	1. System terminates the process (end the chat).	Automatic	Active	3	Child is restricted
			2. System makes the child aware and advises about the danger and consequences of this chat.	Automatic	Active	1	Child is warned.
			3. Informs parents and gives them additional protection options: • allow this activity; • conceal inappropriate chat; • contact their children (voice, text, or video call) to advise them; • blocking (block person, app, Internet use, device); • limit time for using the app	Automatic	Passive	0	Child will be advised by parent, and/or restricted based on parent's decision.

4.3.2 Scenario related to real-world stories of children's exposure to content risks and computer/Interne risks

Children could be exposed to content risk and computer/Internet risks when they use the Internet. Content risks include mature material that is not suitable for children. These inappropriate Internet content could influence children's social and emotional behaviours. Young people often do not realise the difference between reality and fantasy and cannot understand the consequences of violent acts. There is a correlation between repetitive viewing of violence and increased aggressive behaviour, as well as desensitisation to violence (Wallace 2014). For example, CNN related a story of girls who tried to murder their friend because they read and believed in Slenderman and thought that the only way to appease him was to make a blood offering:

> *This story takes a very dark and tragic turn. With the arrest last weekend of two 12-year-old girls in a suburb of Milwaukee for the alleged stabbing and attempted murder of another 12-year-old girl -- their friend.*
>
> *The young suspects were arrested after allegedly luring their innocent friend into the woods and stabbing her. And a criminal complaint says the suspects admitted they were trying to impress "Slenderman," whom they read about on a horror website* (Steyer 2014).

The girls might not have understood that Slenderman is not a real person and were influenced by him. *The Sun* also reported a story of a child trying to kill himself because he had been influenced by a PUPPET YouTube video:

> *A MUM has blamed a popular YouTube video after finding a makeshift noose around her seven-year-old son's neck. He was discovered after his younger brother came downstairs to warn her what was happening.*
>
> *The mother said the youngster claimed to have been inspired by a clip starring a foul-mouthed puppet named Jeffy.*
>
> *She said: "I asked him why he did it and he said he had got it from Jeffy.*
>
> *Apparently Jeffy is the latest craze and all the kids at my son's school love it but they are full of swearing.*

> *They show him as a foul-mouthed, ill-behaved teenager who torments his father, who is played by Super Mario.*
>
> *In the episode which the mum believes inspired her son, Jeffy threatens to kill himself because his dad won't buy him an iPad game. It has been viewed over 12 million times* (Stroud 2017).

Also, children could be exposed to security risks such as malware and phishing through emails attachments or pop-up ads, that could gather sensitive information such as passwords or credit card details. For example, Fortnite scams that offer coupons or codes for free V-Bucks, which actually cost the user his or her personal data or credit card billing information. Young children are not be aware of that scam, and they want to get more V-Bucks so they can purchase characters. Unfortunately, there are around 53,000 complaints from Fortnite users per month according to Epic.com (Miller and Hart 2019).

In these reports above, the children had engaged in risky behaviour, such as reading or watching content that was inappropriate for their age or clicking pop-up ads. The resulted predicted risk from one action could be different depending on activity risk level (action's participation in the occurrence of online risks) and child's individual factors (age, experience, psychological characters, and child's Internet access and use). In the previous incidents, children conducted high risky activities that include accessing an inappropriate content or clicking pop-up ads (High risk activity). Using default values of risk assessment model, if the child conduct high risk activity, the resulted risk value is high even the child is at a high risk level or low risk level.

Overall, the proposed system will monitor a child's activities, computer risk level, and take different actions at different stages depending on the resulted risk value in order to protect the child, as presented in Table 21.

Table 21: System's response to exposure to inappropriate content

Inputs			**Outputs**					**Result with system intervention**
Risky behaviours	**Risky behaviour level**	**Risk value = L×I**	**System intervention and response**	**Auto or manual**	**Active or passive**	**Disruption**	**Stopping power**	
- watching or reading about an inappropriate content. -Clicking on pop-up ads or attachment from unknown people.	H	R=L	Inform parents through report.	Automatic	Passive	0	0	Child is monitored
		R=M	1. System makes the child aware and advises of the danger of this inappropriate content or ads.	Automatic	Active	1	0	Child is warned
			2. Informs parents and gives them additional protection options: • disallow this activity; • filter content; • contact their children (voice, text, or video call) to advise them; • blocking (block app, Internet use, device); • limit time for using the app.	Automatic	Passive	0	0	Child will be advised by parent, and/or restricted based on parent's decision
		R=H	1. System disallows this activity.	Automatic	Active	3	1	Child is restricted
			2. System makes the child aware of the risks of inappropriate content and ads.	Automatic	Active	1	0	Child is warned
			3. Informs parents and give them additional protection options: • allow this activity; • filter content; • contact their children (voice, text, or video call) to advise them; • blocking (block app, Internet use, device). • limit time for using the app.	Automatic	Passive	0	0	Child will be advised by parent, and/or restricted based on parent's decision

4.4 Conclusion

This chapter has presented a novel system that use risk communication to raise awareness of potential risks for parents and give them a granular level of control to manage their child(ren)'s Internet use. The system framework consists of children's applications usage monitor that monitors children's online activities, risk assessor that assesses the risk levels of children's online activities, and a responder that issues the protection responses based on the resulted risk level. A risk assessment method was also proposed that calculates the risk level of children's online activities based on likelihood and impact (severity of harm). The likelihood is evaluated based on children risky online activities and individual factors of children (age, experience, psychological characters, and child's Internet access and use) that could raise the probability of harm to children. Then, the system issues different protection responses to deal with various risk levels (low, medium, and high). In the next chapter, the design and implementation of the prototype system is presented in order to gain insight into its functionalities and how it works.

Chapter 5: Proof-of-concept prototype

A theoretical explanation of the proposed system was presented in the previous chapter. The next phase of the research focused on developing a prototype system that would provide a clear image of the proposed functions and how they could be used. The system was proposed to raise awareness among parents and enable them to understand the potential risks of children's online activities and help them make the right decisions. This chapter describes the implementation of the prototype system and highlights its most important features, which include a risk assessment of children's Internet use, and a granular level of control and adaptation of the protection responses to different risk levels.

5.1 Prototype system implementation overview

Implementing a fully functional system was challenging, due to the need to have the concept first assessed by parents to demonstrate that the system would be useful, usable, acceptable and satisfactory. The programme was further limited by the research time frame. Therefore, the prototype system implementation aimed to produce a proof-of-concept tool and focused on representing the proposed features (i.e., assessing the context of a child's Internet use and customising the protection response to the context). The prototype was developed to work as a system and focus on visualising the proposed functions to be evaluated by parents, while avoiding presenting the existing functions in parental control applications that parents already use.

Most of the existing parental controls offer monitoring and restrictions of the platforms used by children, such as video-sharing platforms, websites, social networking sites, and games that are commonly linked to online risk (content, contact, and conduct risks). The risks associated with video sharing, certain websites, and games are mostly content risks, whereas risks associated with social networking are mostly linked to conduct and contact risks.

The proposed system architecture assesses the risk level involved in children's online activities on the above-mentioned platforms and provides a granular degree of control involving three levels:

1. Parents can assign protection responses for low, medium, and high risk events.
2. Parents can manage risky activities and tailor the protection responses to each activity individually.
3. Parents can manage activities involved on a specific platform (application category).

The system is, therefore, more flexible than the currently available measures. For example, when parents do not want to manage each activity individually, they can assign general protection responses for the child when he/she facing a low, medium, or high risk event, so general protection responses are inherited as a protection response for different activities. On the other hand, if parents are more concerned about specific activities on different applications, they can assign specific protection responses for these activities.

A mobile app wireframe tool (MockFlow) was used to build and form the structure and functionality of the proposed system. It helped in building the interactive mobile app prototype by providing a user-friendly platform with a large library of mock-up components, icons, and other shapes to visualise user interfaces quickly and efficiently. The system provides a user-friendly interface that was designed to be stylistically similar to the existing parental controls presented in section 3.1. The main interface of the prototype system is depicted in Figure 27. Parents can create an account for their child to manage his/her Internet use through the 'Add child' option, by inserting the child's name, gender, date of birth, experience (years online), and psychological characteristics (e.g., sensation-seeking and psychological difficulties). Parents can also complete the Strengths and Difficulties Questionnaire (SDQ) (Goodman et al., 1998) and sensation-seeking questionnaire provided in the system to measure the psychological difficulties of their children.

The system enables parents to manage each child's account individually. In this case, two children's accounts (Emily and William) are assumed and displayed in the interface. The system also presents an option called 'Shared settings', which enables parents to have the same protection response settings for all their children's accounts. In addition, it displays a 'Risk assessment setting' that enables parents to see and assess the effect of the factors related to the child's personality and his/her Internet use context (i.e., the child's age, psychological difficulties, sensation-seeking, Internet experience, access location, type of device used, time online, and frequency of use) that might increase the probability of risk occurrence.

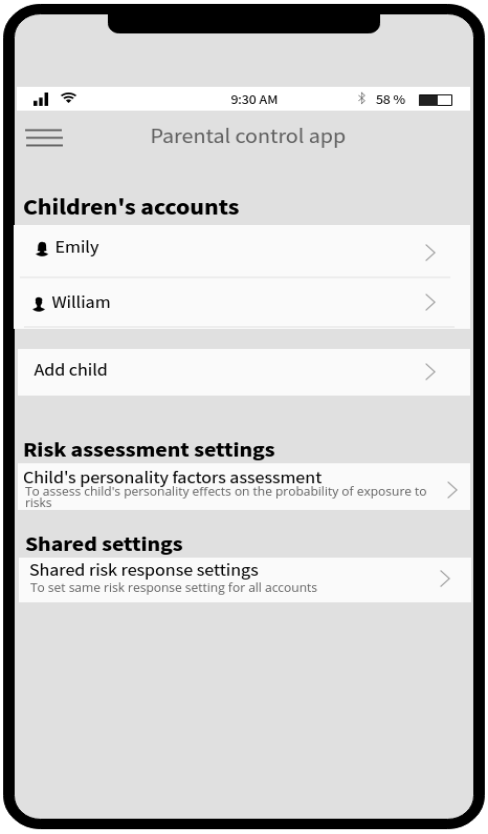


Figure 27: Main interface of the system

Parents can select a child's account to monitor the child's activities and manage the protection responses for that child individually (Emily's account interface is selected in this case and is displayed in Figure 28). The prototype system displays the child's activities summary and offers a monitoring feature (a monitoring function is provided in current parental control apps) to enable parents to monitor a child's online activities. There are three options for monitoring a

child's activities at the top of the interface: a 'View latest questionable activities' option to view a list of risky activities; a 'View activities reports in different application categories' option to view a child's activities in different application categories, such as web, social network, file sharing, and games; and an 'Alert and report setting' option to manage alert and report settings, such as determining parent's email or phone number in order to receive alert or report, and how parents will receive the child's activities report (daily, weekly, or monthly).

The advanced facilities provided by the system assess the risk levels of children's online activities and assign mitigation options that can be activated by clicking on the 'Risk control setting' button. Three levels of protection response are displayed: (a) assigning general protection responses that will be taken when a child is at different risk levels; (b) assessing the questionable activities risk levels individually and customising the protection responses to those activities; and (c) assessing the activities involved on a specific platform (application category).

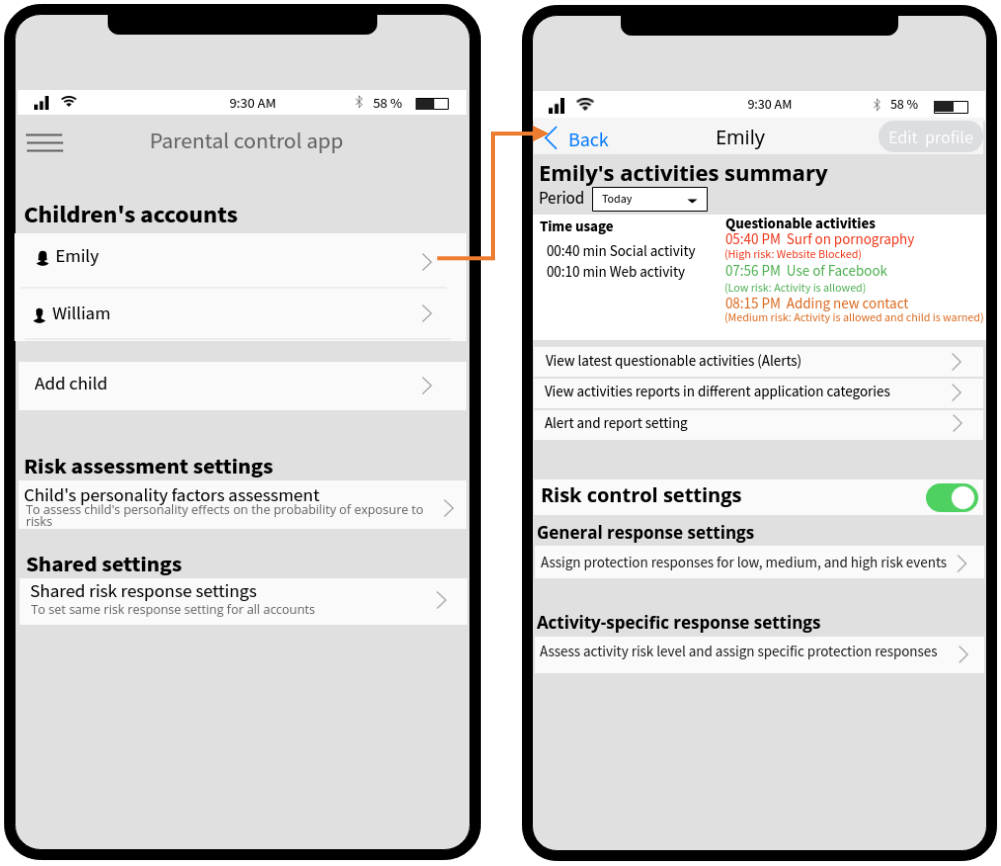


Figure 28: Main interface for managing a child's account (Emily)

5.1.1 Assigning general protection responses

This feature enables parents to assign general protection responses for low, medium, and high risk events (see Figure 29). This feature could save parents time if they prefer not to manage each activity individually. Parents can change and assign appropriate protection responses that will be taken when the child is at a low, medium, or high risk level. General protection response options include the following:

- 'Control the activity': this option enables parents to allow or disallow an action. Parents could also allow the child to request an exception.
- 'Issue awareness-raising for the child by system': this is an option for the system to send a warning message to the child about the risk and consequences of that action and advice about how to avoid the risk in a way that is simple, easy, and understandable for children.
- 'Alert parent immediately': this is an option to send an alert to the parent when the child is at low, medium or high risk, through pop-up notification, SMS message, or email. Parents can also advise and contact the child by text message, voice call, or video call.
- 'Limit application use': this option enables parents to restrict a child's use of an application for a specific duration on particular days (e.g., allowing access for one hour every day), or to a specific time of day (e.g., allowing access from 7 am to 6 pm every day).

Figure 29: Assigning general protection responses for low, medium, and high risk events

5.1.2 Assessing the risk level of questionable activities and customising the protection responses

This feature enables parents to assess the risk level of activities individually and customise the protection responses (see Figure 30). The system facilitates the management of common risky activities that could lead to online risk (content, contact, and conduct risks). The most common risky online activities include: those related to content and commercial risks, which include accessing inappropriate content, downloading applications, and app purchases; and activities related to contact and conduct risks, which include adding a friend, inappropriate chatting, use of a camera/microphone, sharing personal information, and spending a lot of time online. Different online activities can have different risk levels and various impact consequences, which might require different protection responses.

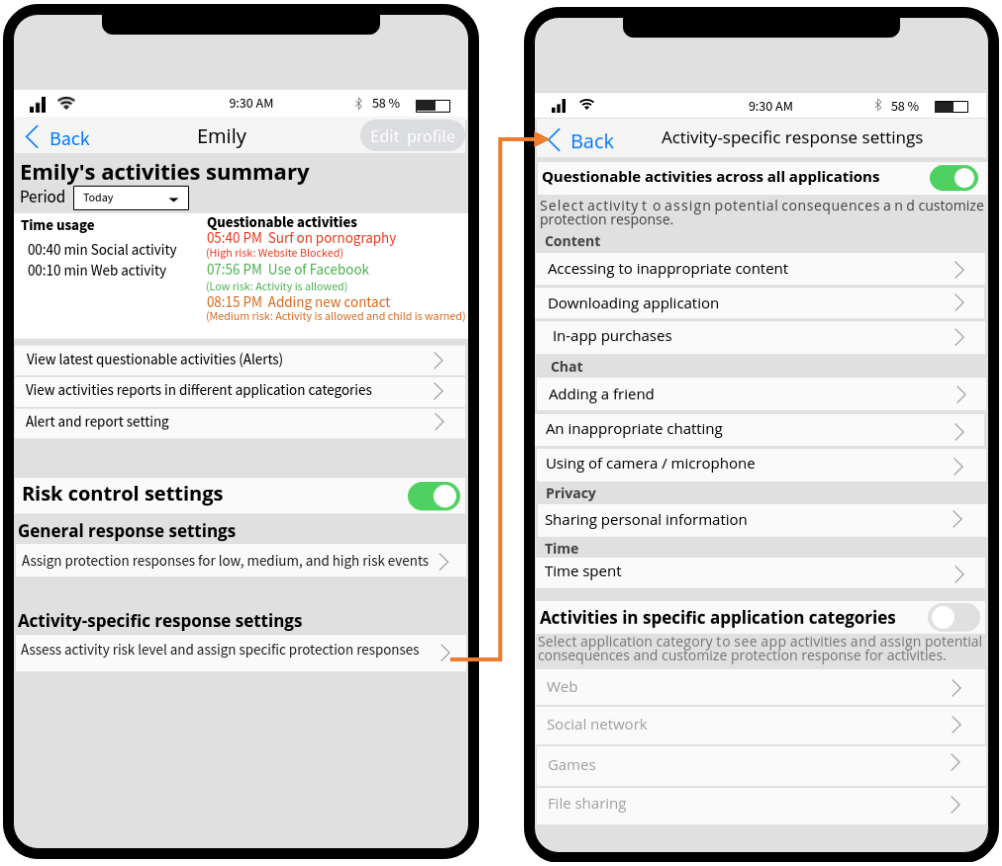


Figure 30: Assessing the risk level of questionable activities and customising the protection responses

For example, if parents select the ‘Accessing inappropriate content’ activity (Figure 31), a list of inappropriate content categories is displayed, so that parents can determine if content is inappropriate for their child. Then the system displays two risky activities related to inappropriate content: ‘Accessing inappropriate content’ and ‘Searching for inappropriate content’, which could have different protection responses (e.g., parents can assign specific responses to searching for inappropriate content, such as enabling a safe search). In this case, if parents select an activity (e.g., Accessing inappropriate content), the risk level of the activity (i.e., default values) and potential consequences (the effect of the activity on the child’s safety, privacy, social relationships, finances, and disruption) will be displayed and the parents can change them. Lastly, the system displays the default protection responses for the predicted risk of the child accessing inappropriate content in order to allow parents to check and edit responses to this activity if they prefer. The response options include general protection responses, such as ‘Control the activity’, ‘Issue awareness-raising for the child by system’, ‘Alert parent immediately’, and ‘Limit application use’; as well as specific protection responses to that activity, such as ‘Filter content’, which reviews the content and limits access to inappropriate content.

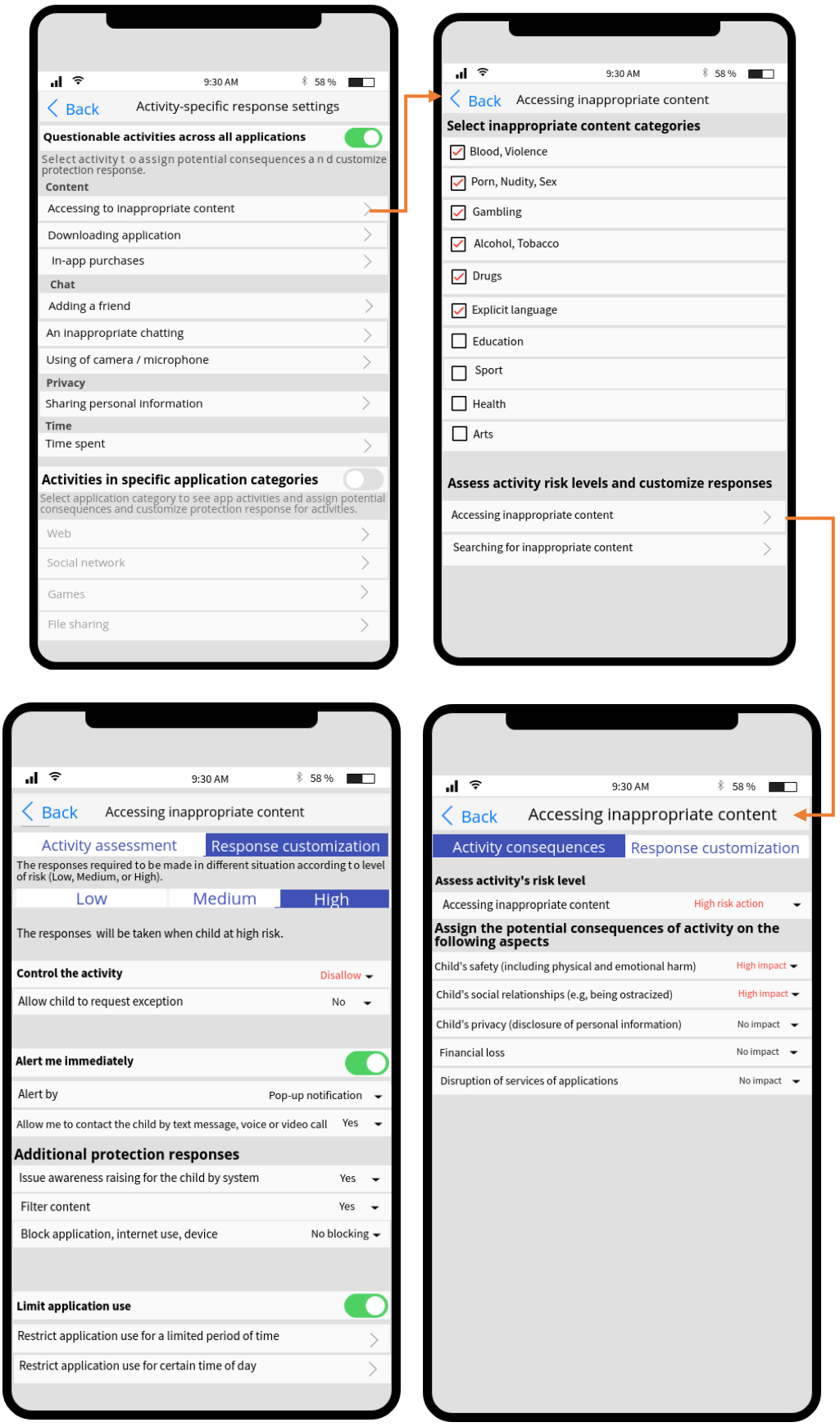


Figure 31: Assessing the risk level of 'Accessing inappropriate content' and assigning protection responses

5.1.3 Assessing the activities involved on a specific platform (application category)

The system also enables parents to manage the platforms that are associated with online risk occurrence individually. It offers a feature to manage activities involved in different application categories, such as web, social networking, file sharing, and games. For example, if parents are concerned about the Web, they can select the web option to manage those activities (Figure 32), such as the use of a web browser, managing access to inappropriate websites, and customising responses.

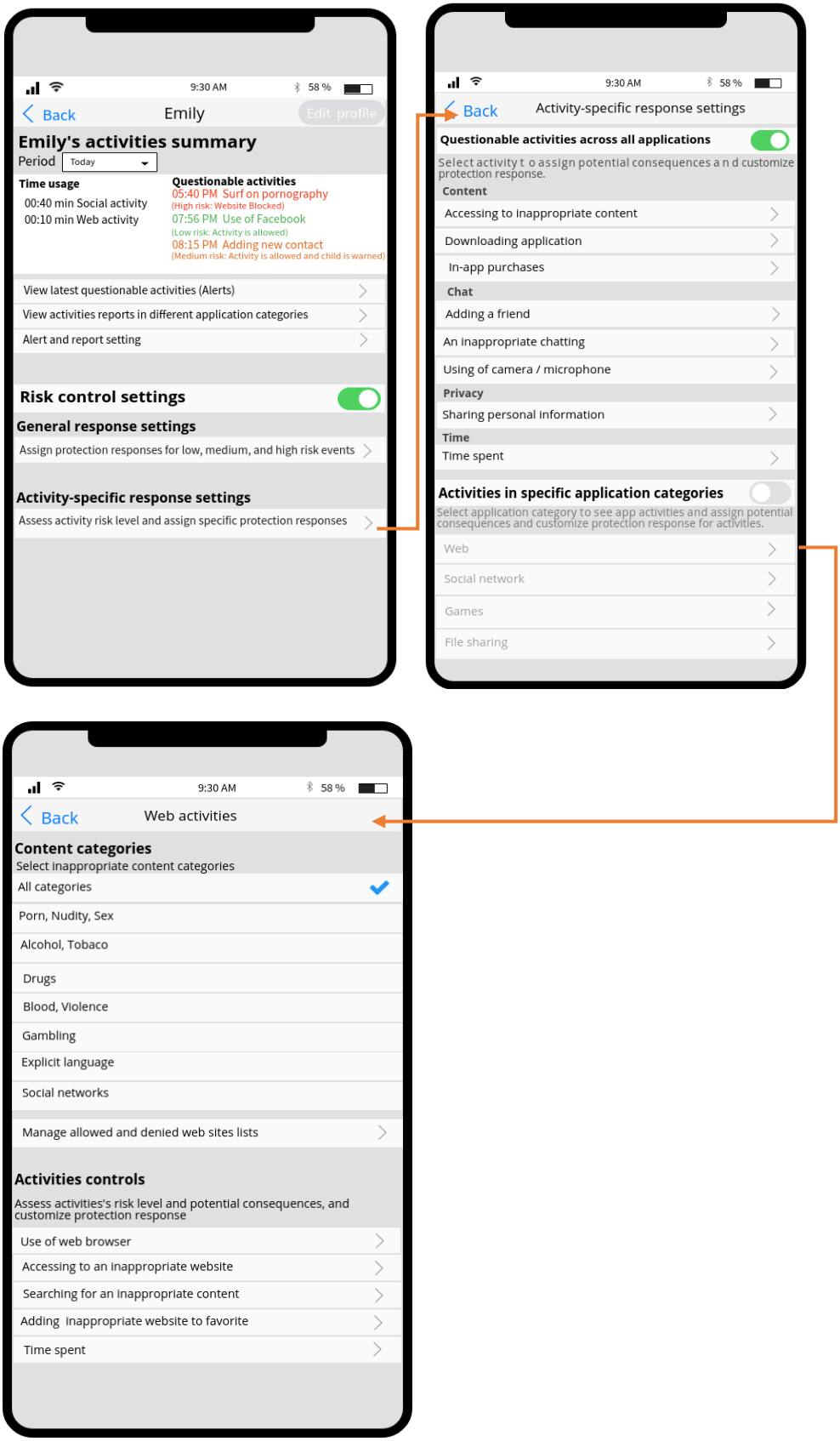


Figure 32: Managing web activities

5.1.4 Simulated alert

Parents might prefer to receive an alert only when their child is at high risk. An example of a simulated alert notification is displayed in Figure 33. The alert gives parents information about the child's activity. In this scenario, the alert refers to the child's risky activity, which was an attempt to access inappropriate content (pornography) and gives the time and date of the access and the number of attempts made to access the website. The system also offers further advice for parents about the potential risk and safeguarding guidance. In addition, the alert informs parents about what the system does in response in order to protect the child (in this case, the child is warned and blocked). Furthermore, the alert offers additional protection responses, such as an 'Allow' option if parents find the website is appropriate for their child and would prefer to allow him/her to access the web; a 'Contact your child' option, which enables parents to advise and contact their children by text message, voice or video call; a 'Limit time' option, which enables parents to set a time limit for using an application, Internet or device; and 'Blocking options', which enable parents to block a web browser, Internet use or a device.

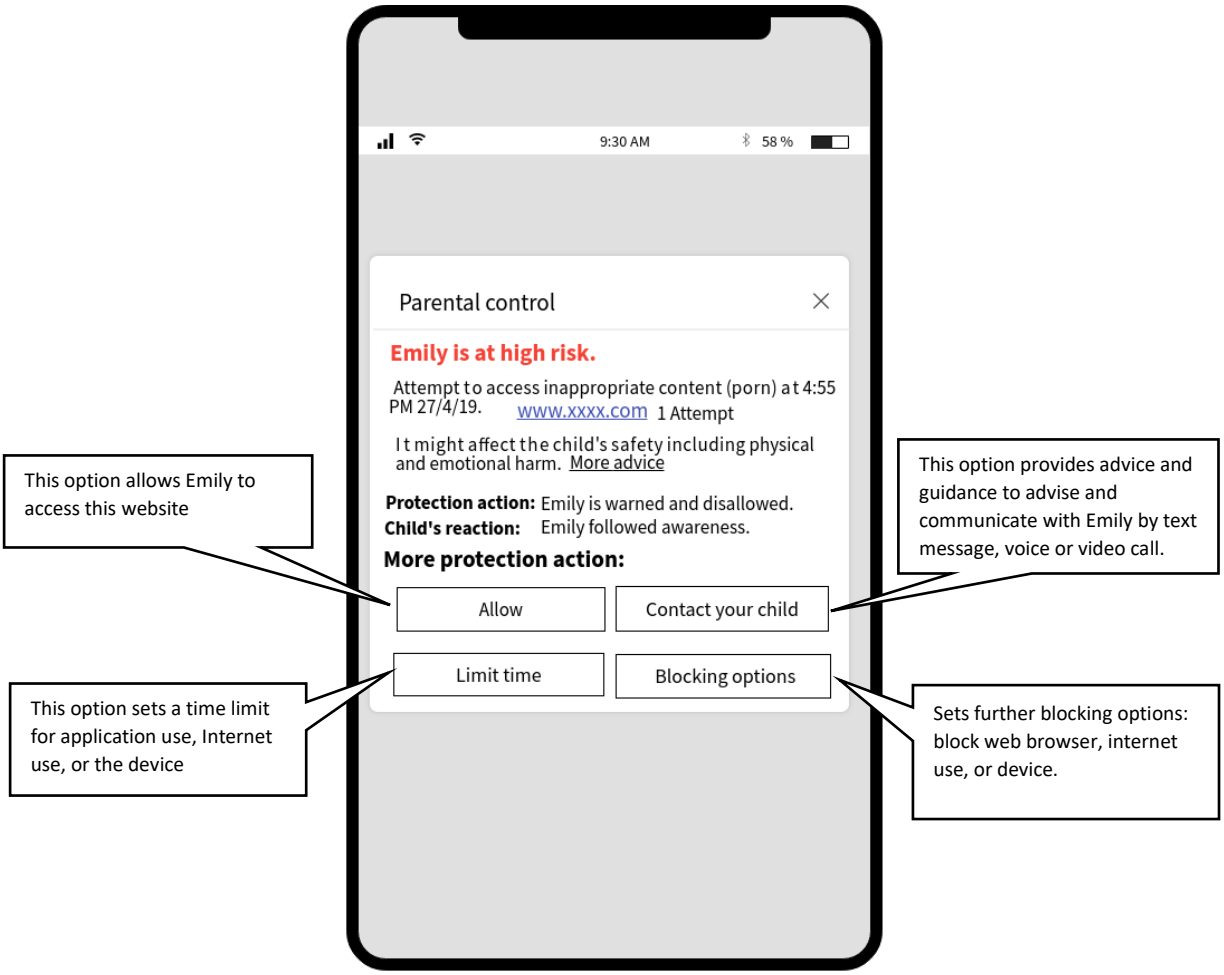


Figure 33: Simulated alert

5.2 Conclusion

This chapter presented the implementation of the prototype system to gain insight into its functionalities and how it could be managed. The prototype system implementation focus on presenting and visualising the proposed features (i.e., assessing the context of a child's Internet use and customising the protection response to the context). The proposed system is more flexible and provides a granular degree of control for parents that involve: assigning general protection responses for low, medium, and high risk events, and also enabling to manage each risky activity individually and assign specific protection responses for these activities. After implementing the prototype system, it is important to evaluate the prototype system to gain parents' feedback about the system. So, the next chapter discusses the evaluation methodology used to assess the usability and usefulness of the system.

Chapter 6: Prototype system evaluation

This chapter presents the evaluation methodology used to assess the usability and usefulness of the prototype system. It identifies the research methods employed for this study and the different methods employed for data collection and procedures, the research participants, and the performance of the data analysis. It also presents the research findings after analysing the data collected by the survey questionnaire and direct observation during the experiment.

6.1 Prototype system evaluation methodology

This section discusses the evaluation methodology used to assess the usability and usefulness of the system. It includes the research method and data collection, participants and sampling, pilot testing, and data analysis techniques.

6.1.1 Research method

The prototype system was developed to simulate the proposed parental control application and give the user a good feel of how the proposed system will work. So, the prototype system was used to evaluate the system at the early stages of system development and give an indication that this system is useful and usable. Thus, the research experiment involved asking parents to use the prototype system and perform certain tasks most signification to the functionality of the system (i.e., assessing the context of a child's Internet use and customising the protection response to the context). Also, participants were asked to think aloud and describe their actions in order to articulate the participants' thoughts and how they perceived and understand the system. In addition, the experiment used some metrics including the task completion rate (participants who complete the task) and task completion time (the time that the participant took to perform the task). So, the experiment enabled to identify the participants' impressions about the system and potential usage difficulties. Also, the experiment involved pre-test questionnaire that designed based on EU Kids Online research network which focused on investigating

children' online usage, parents' concerns and use of parental controls, which was useful for the interpretation of the parents' interaction during the experiment. In addition, a post-test evaluation questionnaire was used to gain feedback about parents' satisfactions about the system. So, the experiment results can provide indication about participants' satisfactions, and perceived ease of use, and provide recommendations and directions for the modification and any improvements of the system that may need to be undertaken.

At the beginning of the experiment, the participants were given an introduction about the research and experiment objective and asked to sign a consent form. Then, the participants were asked to complete an online survey about their children's Internet use and their use of parental mediation. Then, the participants were presented with the system's home page, and were asked to use the tool so that they could familiarise themselves with the system interfaces. They were then asked to perform a set of predetermined tasks: (a) assigning general protection responses that will be taken when a child encounters different risk levels; (b) assessing the risk level of questionable activities individually and customising the protection responses to those activities; and (c) viewing an alert notification of a child's inappropriate online activity and giving their opinion of whether the alert was useful and efficient. Table 22 lists the task scenarios used in the evaluation and the sequence of steps required to complete the tasks. The participants were asked to 'think aloud' to know what they were doing and the experimenter observed the participants while they performed the tasks. After completing the tasks, the participants were also asked to complete an online survey to gain feedback about the system's usefulness and usability and any desirable additional functionality.

Table 22: Usability scenarios

Task	**Description**	
Task 1	**Scenario**	*In this scenario, you are the parent of 12-year-old Emily, who uses the Internet and could be at different risk levels (low, medium, or high).*

		You are concerned about Emily and you want to know the protection responses for high-risk events. *Please use the system to access Emily's account:* • *Check the general risk response(s) assigned for a high-risk event (such as allowing the child's activity, receiving an alert, issuing awareness-raising for the child, and limiting application use). If you are not happy with the default protection response(s), you can change them.*
	Task completion steps	To complete the tasks, the participant had to: 1. Select the child's account: "Emily". 2. Select "Assign protection responses for low, medium, and high risk events". 3. Choose a high risk event to assign protection responses. The scenario ends with the user assigning appropriate protection responses to a high risk event.
Task 2	**Scenario**	*In this scenario, you are concerned about Emily's activities, such as accessing inappropriate content. Thus, you want to assess the risk level of accessing inappropriate content and want to know the protection responses for this activity.* *Please use the system to access Emily's account and activity-specific settings.* • *Check the current risk level setting of general access to inappropriate content (low, medium, or high) and impacts (such as the child's safety, the child's social relationships, the child's privacy, financial loss, and disruption of services). If you are not happy with the default settings, you can change them.* • *Check the assigned protection responses for this activity (such as allowing the child's activity, receiving an alert, issuing awareness-raising for the child, filtering content, and limiting application use). If you are not happy with the default settings, you can change them.*
	Task completion steps	To complete the tasks, the participant had to: 1. Select the child's account: "Emily". 2. Select "Assess activity risk level and assign specific protection responses".

		3. Select activity: "Accessing inappropriate content". 4. Determine inappropriate content category. 5. Assess activity's risk level and impact consequences. 6. Determine appropriate protection responses. The scenario ends with the user assessing the activity's risk level and assigning appropriate protection responses.
Task 3	**Scenario**	*In this scenario, you received an alert informing you that Emily is at risk in order to warn you of the risky activity and to offer responses in order to avoid risk. Please consider the alert and answer the following questions:* • *Do you feel that you generally understand the alert?* • *What did Emily attempt to do that caused the alert?* • *What did the system do in response in order to control the activity?* • *What additional protection option(s) do you have?* • *Do you understand the options available to you?* • *Do you have any further comments?*

The experiment was conducted on a Huawei tablet with each participant individually at the University of Plymouth (Centre for Security, Communications and Network Research, or CSCAN). The participants' performance of tasks was recorded in order for this to be reviewed in later analysis. Although a time slot of 60 minutes was reserved for each session, this was not regarded as a limit, as it was expected that some participants would need more time to complete the experiment than others. Generally, the whole experimental process lasted approximately 43 minutes.

6.1.2 Data collection methods

The research approach involved a mix of qualitative and quantitative methods. It was felt by the researcher that collecting, analysing, and mixing both quantitative and qualitative data could provide a better understanding of usability problems and system usefulness. Quantitative data were gathered from the survey questionnaires (a pre-test questionnaire to collect data about the parents' concerns and use of parental mediation of children's Internet use, and a post-test

evaluation questionnaire to collect data about the parents' level of satisfaction with the system). Qualitative data were collected from observations (observing parents' interaction with the proposed system). Both quantitative and qualitative data were analysed in order to discover any significant findings. The techniques employed for collecting data included a talking/thinking aloud protocol and observations and questionnaires.

6.1.2.1 Talking/thinking aloud protocol and observations

A thinking aloud approach with observations is a quantitative data collection method that is used in practical evaluations of human-computer interfaces. In this experiment, the participants were asked to talk aloud and describe their actions as they completed the tasks, in order to articulate their thoughts and how they perceived the system for the researcher. These 'verbal thoughts' from the participants enabled the researcher to determine and understand both what the participants were doing and why they were doing it.

The observation method was used to collect data about the behaviour and actions of the participants while they interacted with the system and completed the assigned tasks. Observation data were used to supplement the data provided by the talking aloud method in order to fully understand the situation (what they said they were doing and what they did). Observation is used to collect information relating to instances in which participants seem to be confused (i.e., difficulties and problems encountered by participants).

6.1.2.2 Questionnaires

Survey questionnaires enable participants to complete their responses at their own convenience. Questionnaires gather feedback from each participant about predefined questions that can be balanced with the feedback from other methods. In this study, two types of questionnaire were completed: a pre-test survey and a post-test survey.

A pre-test survey was completed at the beginning of the experiment to collect parents' demographic data, their children's demographic data, and information about the children's

Internet use and the parental mediation used (Appendix C). This questionnaire provided insight into parents' concerns about their children's Internet experiences and how they managed their children's Internet usage. It aimed to gather information about the background of the parents about their children's Internet use, which was useful for the interpretation of the data collected during the experiment. The feedback from this questionnaire was employed to measure the effects of the participants' background on their interaction with the system.

The post-test survey was completed at the end of the experiment and had the aim of gaining participants' feedback on their perceptions of the system's usefulness and usability (Appendix D). The survey collected qualitative and quantitative data that provided feedback about the participants' experiences of the system and their satisfaction levels. It consisted of closed as well as open questions. Closed questions were used to gather quantitative data and provide numeric representations of participants' satisfaction with the system interface design and functions, ease of use, and intention to use, using a five-point Likert scale. Open questions were used to generate qualitative data and gain more unique and varied insight into the subjects' experiences and what they liked/disliked about the system.

6.1.3 Research participants

The parental control application was assessed by parents who were deemed to be representative of a typical user of that application, in order to collect their perceptions and opinions of the system's effectiveness and usability. The participants were chosen as they were parents of children aged between 4 and 16. In order to recruit participants to the experiment, an invitation email was sent to University of Plymouth employees and a £15 payment was offered for participants upon completion of the study. An invitation was also distributed in schools, nurseries, and churches. The invitation provided information about the proposed system and experiment procedure and the total amount of time needed for the experiment. After those who responded had agreed to take part in the experiment, the time of the experiment was arranged in accordance with their availability and they were informed where to attend for the session.

Ethical approval was also taken into consideration and participants were informed that their information would be treated confidentially and that data would be anonymous during the collection, storage and publication of the research material. The sample size intended for the evaluation study was 35 parents, as it would have been difficult to gather a vast amount of data from a large sample due to time and cost. As the research employs a mixed evaluation approach, treating a large sample would have been very costly and time consuming.

Five of the participants took part in a pilot test and 30 participants were taken into the evaluation process. The participants in the study were nine males and 26 females. The majority of the participants were from the UK (27), and the remainder were as follows: 1 (Ukraine), 3 (Saudi Arabia), 1 (Ireland), 1 (Algeria), 1 (Iraq), and 1 (Greece). The majority of the participants also had a university-level education and were frequent Internet users. (The ethical approval letter, research information sheet, consent form, and invitation are included in Appendix A.)

6.1.4 Pilot test

Prior to conducting the main evaluation study, a pilot test was carried out in order to observe the experimental procedure, including the time needed for the experiment, participants' interactions with the system interfaces and tasks, and the methods of data collection. The pilot test was first undertaken by the two research supervisors, Dr Shirley Atkinson and Dr Maria Papadaki, and five participants. The pilot study enabled an estimation of how long participants might take to complete the experiment: the time for the whole session was between 20 and 48 minutes, the time taken to complete the first task was between 1 and 4 minutes, and the time taken to perform the second task was between 3 and 8 minutes.

The pilot test helped to track the pilot test users' interactions with the system and identify difficulties and problems in order to refine the system interfaces, tasks, and questionnaire. The system interfaces were refined in order for them to be simple and clear. An explanation was added for each option presented in the system interfaces regarding the facility provided by the

option. For example, an explanation was added below the "General risk response setting" option to show that the option could be used for managing the response to any event that has a low, medium, or high risk level, and so on, as displayed in Figure 34. The child's activities summary could also indicate recent risky activities and the responses taken, which might help participants to know and understand that different activities have different risk levels and need different responses. The interface also displayed options for managing risky activities related to content, chat, and privacy; thus, it was felt that it might be better to simplify the interface and clarify the risky activities by showing the activities directly, as shown in Figure 35.

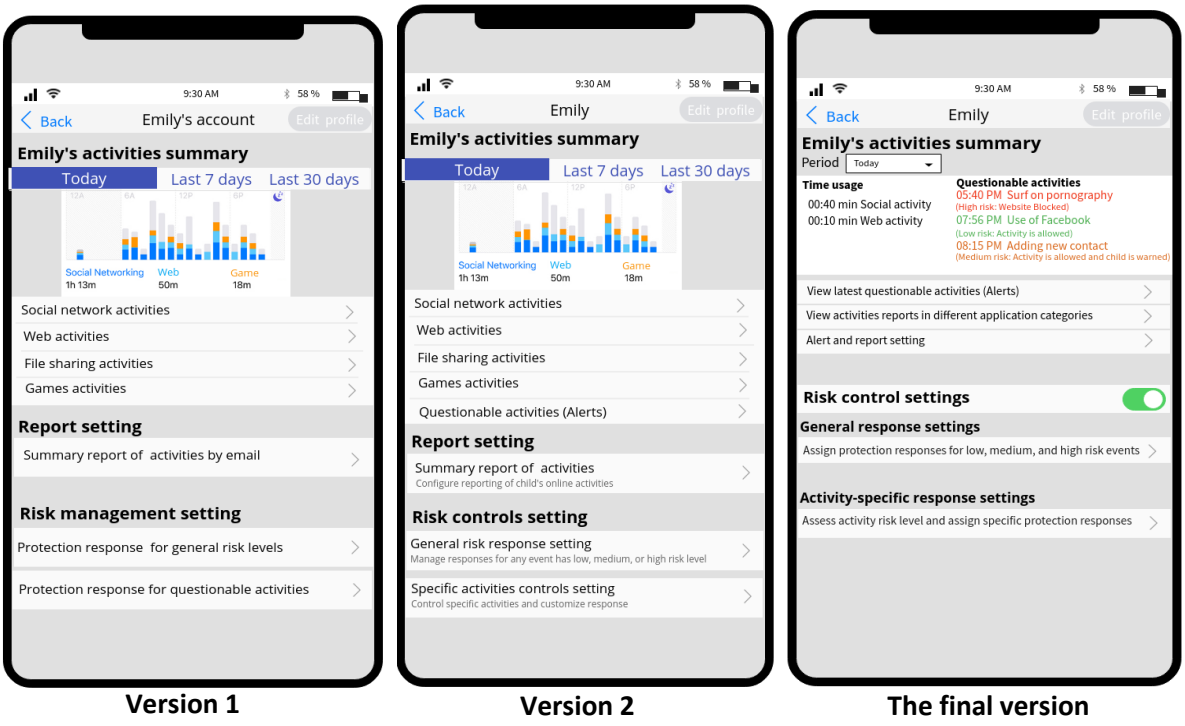


Figure 34: Changes to the main interface for managing the child's account

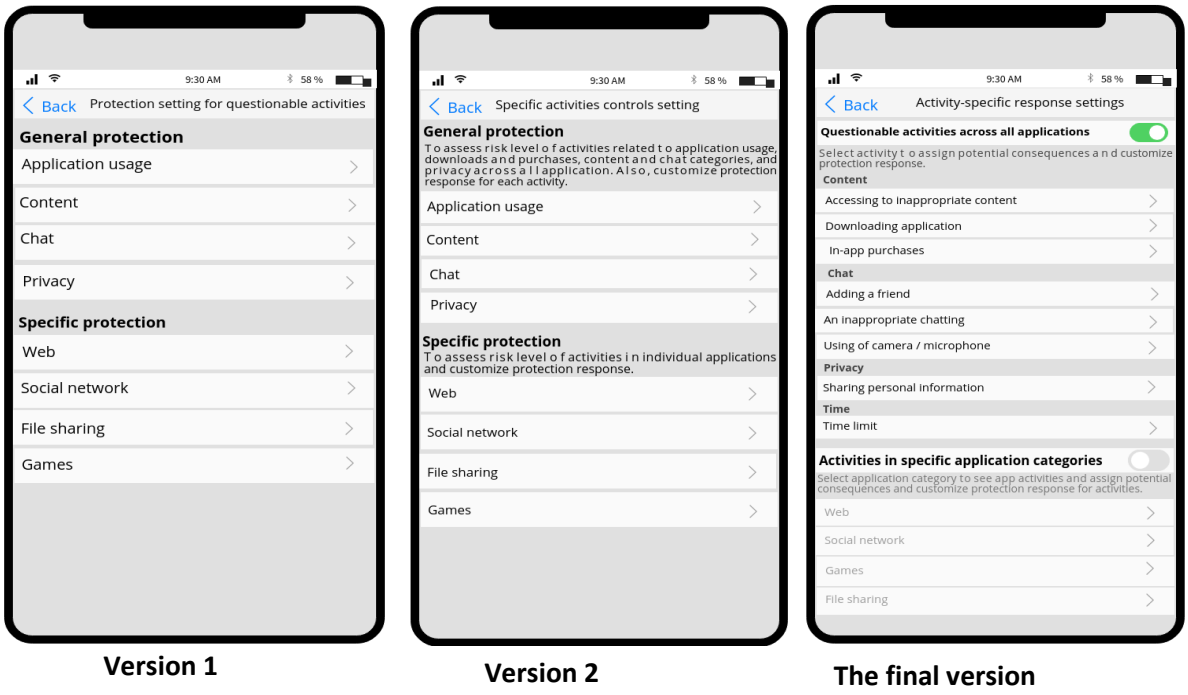


Figure 35: Changes to the interface for managing risky activities

With regard to task description, it was felt that the task could be clearer and direct the participants more effectively by avoiding the introduction presented in the tasks, which could confuse users and waste time (see Appendix B for detailed changes). Asking participants to perform a task without giving them an opportunity to use and explore the system could also be a challenge for them. Thus, it was useful to ask the participants to use and browse the system before doing the tasks in order for them to become familiar with the system interfaces.

In relation to the questionnaire, some questions were reconsidered in order to gain and understand the participants' perspective. For example, participants were asked about their concerns regarding their children's Internet use in general and then had to respond regarding their concerns about the children's online activities individually. However, while some participants might not be concerned in general, they might express concern when they thought about each activity (see Appendix C for the detailed changes). Some participants considered certain online activities as being high risk but were not concerned because they monitored their children or trusted them. Therefore, some questions were added to the questionnaire to ask the

participants about the risk levels of common online activities and the impact consequences of those activities, as these could differ according to the parents' views and experiences with their children at different ages. Furthermore, the pilot test allowed the experimenter to practise the experiment with a small group before the main evaluation, which provided the experimenter with reassurance with regard to administering the experiment.

6.1.5 Data analysis

System usability and usefulness testing required collecting both the participants' performance (objective measure) and level of satisfaction (subjective measure). Performance measures were related to the participants' actions and behaviours and could be collected from observations of the participants' interaction with the system. The performance measures used were the task completion rate and the task completion time. The task completion rate was defined as the number of participants who completed the task without assistance. Some participants encountered difficulties and felt confused and thus needed assistance to understand and complete the task. Difficulties might have been related to the participants' concerns and familiarities with the domain (pre-survey data were used to identify patterns and connections between the participants' background and their performance). Task completion time was the time a participant took to perform the task.

Participants' satisfaction was related to their perceptions and opinions of the system (i.e., overall satisfaction with the system) and were collected from the post-survey. This measure evaluated participants' satisfaction, attitudes and feelings towards the system and their interactions with it.

6.2 Prototype system evaluation findings

This section presents the study findings after analysing the data collected from the questionnaire and direct observations during the experiment. Pre-survey data are first analysed to gain insight into parents' concerns about and mediation of their children's Internet use. The participants' performance and interactions with the system are then analysed and presented depending on their concerns and experience (participants' background). Lastly, the chapter presents the results regarding the participants' perspectives and satisfaction with the system.

6.2.1 Participants and their children's Internet use data

The pre-survey provided information about children's Internet access and usage and any parental mediation used. It provided insight into parents' perceptions and concerns about their children's Internet experiences and how they managed their children's Internet usage, which was useful for the interpretation of the data from the experiment. Certain aspects related to children's personality data, such as gender and psychological characteristics (psychological difficulties, sensation-seeking) were asked about in the pre-survey. However, the small number of responses was not enough to examine in order to gain a valuable result.

6.2.1.1 Participants' children's Internet access and use

Children's Internet experiences could be affected by conditions relating to the child's Internet access and use. Children's Internet access includes the device used to access the Internet (e.g., shared/own handheld device, shared/own laptop, shared/own desktop computer) and places where children go online (e.g., private room, public place, including a public room in the home or school, and other general places). Children's Internet use includes the age when the child first went online and the frequency of going online. Participants' children's Internet use and access are shown in Table 23.

Internet access and use diversified depending on the age of the child. The majority of the youngest children aged 4-7 used shared devices, such as a handheld device or laptop, to access

the Internet several times a week in public places; thus, younger children were less frequent users. Children were also going online at younger ages: the average age of first Internet use was four for the youngest group. In addition, most of the children aged 8-12 used shared devices to access the Internet several times a day in private and public places, and had started to use the Internet at a younger age (five years old). In comparison, the majority of the oldest children, aged 12-16, used their own handheld devices to go online several times a day in private and public places, and the average age of first Internet use was nine. Overall, the average age of first Internet use was seen to be dropping, with the youngest children starting to use the Internet at a younger age. Ownership of devices also increased with age, as the older children were more likely to have private devices than the younger ones, which might expand the range of places for Internet access with more use and more opportunities, and the more likely risks are to be encountered.

Table 23: Participants' children's Internet usage

Children's Internet access and use		**Children's age**		
		4-7 (Total: 12)	**8-11 (Total: 4)**	**12-16 (Total: 14)**
Device type	Shared handheld device	9	3	2
	Own handheld device	4	1	12
	Shared laptop		2	6
	Own laptop	1		4
	Shared desktop computer	2		2
	Own desktop computer			1
Location	Private room			2
	Public place	12		
	Private and public places		4	12
Frequency of use	Several times a day	3	3	13
	Several times a week	9	1	1
Age of first Internet use	Average age of first use	4	5	9
Total		12	4	14

6.2.1.2 Participants' children's online activities

Children of different ages engaged in different online activities, some of which could expose them to online risks. Table 24 shows children's online activities by age. As the range of online activities varies for the different age groups, changes in opportunities could be related to variations in the experience of risk. Most of the children used a web browser (77%) and communication platforms (60%), played multiplayer games (63%), and had made an app purchase (50%). Online activities increased with age, younger children spending time using the Internet for browsing the Web and playing multiplayer games, whereas most of the older children spent time using the Internet for a variety of online activities, including browsing the Web, using social networks and file-sharing platforms, and playing multiplayer games. On the other hand, a minority of children were engaged in risky activities, such as accessing inappropriate content (23%), accepting people as friends without knowing them offline (27%), inappropriate chatting with people (10%), using a camera/microphone with unknown people (16%), sharing personal information with unknown people (7%), and downloading inappropriate applications (17%). The majority of the children who conducted risky activities were older. Overall, when children grew older, they undertook a wider range of online activities, so they might be engaged in riskier activities.

Table 24: Participants' children's online activities by age

Children's online activities	**Children's age**									**Total engagement in online activities (%)**
	4-7 (Total: 12)			**8-11 (Total: 4)**			**12-16 (Total: 14)**			
	Yes	**No**	**Don't know**	**Yes**	**No**	**Don't know**	**Yes**	**No**	**Don't know**	
Using web browsers	5	7	0	4	0	0	14	0	0	77
Using communication platforms (e.g., social networks, chatrooms, or email)	2	10	0	2	2	0	14	0	0	60
Playing multiplayer games	4	8	0	4	0	0	11	3	0	63
Using file-sharing platforms	0	0	0	1	2	1	10	3	1	37
Making an app purchase	2	9	1	3	1	0	10	4	0	50
Accessing inappropriate content	1	10	1	0	3	1	3	6	5	23
Accepting people as friends without knowing them offline	1	11	0	2	2	0	5	8	1	27
Inappropriate chatting with people	0	0	0	1	3	0	2	8	4	10
Sharing personal information with unknown people	1	10	1	0	3	1	1	10	3	7
Using a camera/microphone with unknown people	1	10	1	1	2	1	3	8	3	16
Downloading inappropriate applications	2	10	0	1	3	0	2	10	2	17
Spending too much time on the Internet	6	5	1	4	0	0	12	1	1	73

6.2.1.3 Participants' assessment of the risk level of children's online activities and impact consequences

Some activities could expose a child to online risk. Children's online activities have different risk levels based on their participation in risk occurrence. Table 25 shows the risk levels of common online activities according to the participants' views. Participants thought about these activities sensibly and were likely to have assessed the risk levels based on their views and experiences. Using a web browser was, for example, considered as low risk activity by one third of the parents and a medium-level risk activity by nearly one third. Using communication platforms was considered to have a high risk level by half the parents, and assessed as a medium risk activity by nearly one third. Almost half the participants assessed playing multiplayer games and using file-sharing platforms as medium risk activities. Online purchasing was assessed as a medium risk activity by nearly half the parents, and one third of the parents considered it a low risk activity. Nearly half the participants assessed accepting unknown people as friends as a high risk activity, whereas more than half the participants assessed accessing inappropriate content, inappropriate chatting, use of a camera/microphone, and sharing personal information as high risk activities. In addition, downloading inappropriate applications was considered a high risk activity by more than one third of the parents, and considered a medium risk activity by one third of the parents. Nearly half the parents assessed the time spent online as a medium risk. Overall, the parents reported using file sharing, playing multiplayer games, making online purchases, and the time spent online as medium risk activities, and reported accessing inappropriate content, using communication platforms and communicating with unknown people as high risk activities, as shown in Figure 36.

The risk levels of the activities were assessed by 30 parents with different concerns about their children at different ages. The activities risk level might differ depending on the child's age, which might be clearer and more noticeable with a large sample of participants. The participants' activities risk level assessment for each age group is presented in Appendix E.

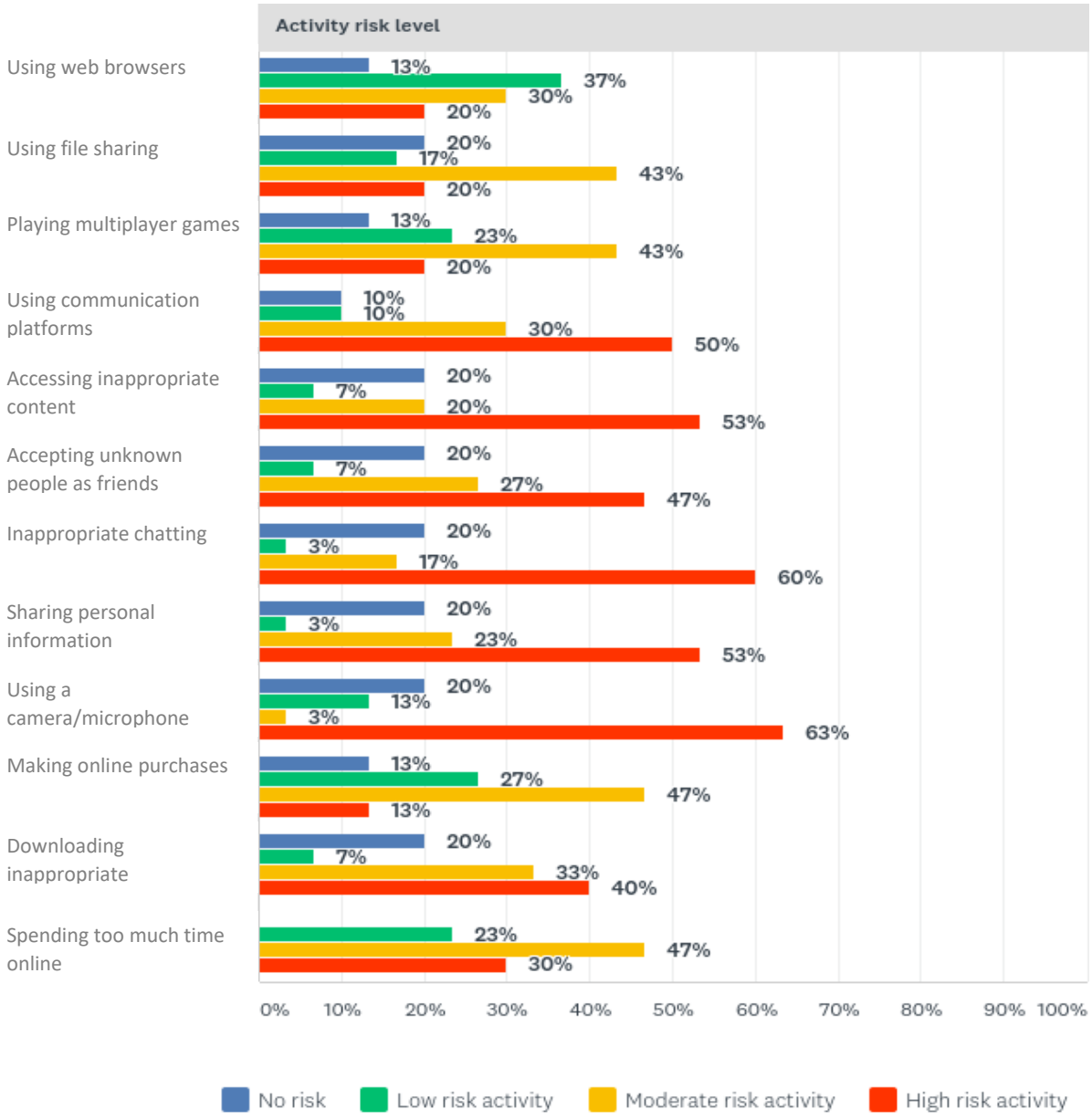


Figure 36: Participants' assessment of the risk levels related to online activities

Table 25: Participants' assessment of the risk levels of online activities

Activities	Activity risk level according to the parents' view				Activity risk level (mode)
	No risk	Low risk	Medium risk	High risk	
Using web browsers	4	**11**	9	6	Low
Using communication platforms (e.g., social networks, chatrooms, or email)	3	3	9	**15**	High
Playing multiplayer games	4	7	**13**	6	Medium
Using file-sharing platforms	6	5	**13**	6	Medium
Making an app purchase	4	8	**14**	4	Medium
Accessing inappropriate content	6	2	6	**16**	High
Accepting people as friends without knowing them offline	6	2	8	**14**	High
Inappropriate chatting with people	6	1	5	**18**	High
Sharing personal information with unknown people	6	1	7	**16**	High
Using a camera/microphone with unknown people	6	4	1	**19**	High
Downloading inappropriate applications	6	2	10	**12**	High
Spending too much time on the Internet	0	7	**14**	9	Medium

Each activity could have different impact consequences for a child, including the following: child safety, social harms (e.g., loss of friends, being ostracised), invasion of privacy, disruption, or financial loss. The type of impact differed depending on the parents' views (i.e., on whether the person initially thought that there was a problem that bothered him/her). Table 26 shows the impact consequences of common online activities according to the parents' views. Parents thought about these activities and assessed the impact consequences of each activity based on their thoughts and understanding. In relation to web browser usage, more than one third of the parents felt it could have a high impact on a child's safety, and more than half the parents thought it could have a high impact on a child's privacy (some websites can track the user's location). Using file-sharing platforms was considered by more than half the parents to have the potential to have a high level of effect on a child's privacy, and nearly half the parents considered that it could have a high impact on a child's safety and social relationships. As considered by nearly half the parents, playing a multiplayer game could have a high impact on a child's safety, social relationships, and privacy. In addition, the majority of parents felt that using communication platforms, accessing inappropriate content, accepting unknown people as

friends, inappropriate chatting, and using a camera/microphone could have a high effect on a child's safety, social relationships, and privacy. The majority of the parents thought that sharing personal information could have a strong effect on a child's safety, social relationships, and privacy, and more than half felt it could also lead to financial loss. The majority of the parents also felt that making online purchases could lead to financial loss. More than half the parents thought that downloading inappropriate applications could have a high impact on a child's safety and privacy and could cause financial loss. Finally, the majority of the parents felt that spending a long time online could have a high impact on a child's social relationships. Overall, parents assessed the impact consequences of online activities based on their perspectives of whether the online activities could cause a problem and affect their children at different ages.

Table 26: Activities impact assessment by participants

Activities	**Impact**																			
	Child's safety				**Child's social relationships**				**Child's privacy**				**Financial loss**				**Disruption of services or applications**			
	No	**L**	**M**	**H**	**No**	**L**	**M**	**H**	**No**	**L**	**M**	**H**	**No**	**L**	**M**	**H**	**No**	**L**	**M**	**H**
Using web browsers	2	7	9	**12**	4	5	**13**	8	2	7	5	**16**	6	**12**	8	4	5	**17**	5	3
Using communication platforms (e.g., social networks, chatrooms, or email)	0	4	4	**22**	0	4	4	**22**	0	4	5	**21**	4	**16**	5	5	6	**13**	8	3
Playing multiplayer games	1	7	10	**12**	0	4	**13**	**13**	0	7	9	**14**	5	7	**12**	6	6	**15**	6	3
Using file-sharing platforms	2	3	11	**14**	2	8	6	**14**	1	5	6	**18**	5	8	**9**	8	5	**12**	8	5
Making an app purchase	1	**13**	11	5	2	**19**	6	3	2	8	**13**	7	1	1	6	**22**	3	5	**14**	8
Accessing inappropriate content	0	2	4	**24**	0	1	6	**23**	0	3	4	**23**	4	8	6	**12**	5	9	5	**11**
Accepting people as friends without knowing them offline	0	0	3	**27**	0	1	9	**20**	0	2	2	**26**	4	5	6	**15**	6	**10**	4	**10**
Inappropriate chatting with people	0	0	1	**29**	0	1	4	**25**	0	1	3	**26**	2	9	8	**11**	6	**10**	5	9
Sharing personal information with unknown people	0	0	1	**29**	0	1	10	**19**	0	0	1	**29**	2	2	9	**17**	5	6	7	**12**
Using a camera/microphone with unknown people	0	1	1	**27**	0	1	8	**21**	0	1	1	**28**	4	9	6	**11**	3	**12**	6	8
Downloading inappropriate application	0	3	9	**18**	0	8	9	**13**	0	3	9	**18**	3	1	7	**19**	3	3	11	**13**
Spending too much time on the Internet	0	6	**12**	**12**	0	1	5	**24**	1	6	7	**16**	3	**13**	12	2	3	**14**	9	4

6.2.1.4 Participants' concerns about their children's Internet use

Results relating to participants' concerns about their children at different ages are shown in Table 27. Parents differed in their concerns about their children at different ages. The majority of the parents of young children were concerned about their children's Internet use, even though younger children are less frequent users and tend to use shared devices in public places. The parents' concerns about their younger children might be because younger children lack safety skills, as well as critical thinking and social abilities. In comparison, half the parents were not concerned about their older children's Internet use, although the other half did have concerns in this respect. Although older children used the Internet more with a wider range of technologies in more places, the parents' concerns differed depending on their experience with their older children's Internet use.

Table 27: Participants' level of concern about their children's Internet use at different ages

	Parents' level of concern		
Children's age	**Not concerned**	**Somewhat concerned**	**Very concerned**
4-7	2	9	1
8-11	2	2	0
12-16	7	6	1
Total	11	17	2

In addition, parents who described themselves as not being concerned already monitored their children. Some parents were not concerned as they trusted their children and used active mediation to discuss Internet safety with them, as illustrated in Table 28.

Table 28: Reasons parents were not concerned about their children's Internet use

Parents' comments about why they were not concerned
"Concern has lessened as he has become older."
"I don't have any concerns as I feel my child is honest with what she looks at online."
"Not concerned with her but others i.e., peer groups, etc."
"We discuss Internet safety, he is aware of the risk, such as disclosing personal information and online grooming, I monitor what he is using."
"We have regular chats about safety, I am added to their friend list so can see the volume of their activity and have set up parental controls."
"I have parental controls and regularly check what is being watched/played."
"I monitor it closely and any apps that she has, I do as well."
"Because I know what she uses on the Internet."

The participants were also asked about their concerns regarding online activities, as shown in Table 29. Generally, more than half the parents were concerned about their children's online activities. The majority of the parents of the youngest children were concerned about most of their children's online activities. In comparison, around half the parents of the older children were concerned about their children's online activities.

Table 29: Participants' concerns about their children's online activities

Children's online activities	Children's age						Total parental concern about each activity (%)
	4-7 (Total: 12)		8-11 (Total: 4)		12-16 (Total: 14)		
	Concerned	Not concerned	Concerned	Not concerned	Concerned	Not concerned	
Using web browsers	7	3	0	4	5	9	40
Using communication platforms (e.g., social networks, chatrooms, or email)	8	4	2	2	10	4	67
Playing multiplayer games	7	5	1	3	8	6	53
Using file-sharing platforms	7	5	1	3	9	5	57
Making an app purchase	10	2	1	3	3	11	47
Accessing inappropriate content	9	3	3	1	9	5	70
Accepting people as friends without knowing them offline	9	3	2	2	8	6	63
Inappropriate chatting with people	9	3	3	1	8	6	67
Sharing personal information with unknown people	10	2	3	1	7	7	67
Using a camera/ microphone with unknown people	9	3	3	1	6	8	60
Downloading inappropriate application	10	2	2	2	7	7	63
Spending too much time on the Internet	11	1	1	3	11	3	78

Although some of the parents were not concerned in general, they expressed concern when thinking about each activity, as shown in Table 30. Around half the parents were concerned about specific activities, such as using social networks, accessing inappropriate content, accepting people as friends without knowing them offline, inappropriate chatting with people, sharing personal information with unknown people, downloading inappropriate application, and spending too much time on the Internet.

Table 30: Participants' concerns about each activity (parents not generally concerned)

Children's online activities	**Concerned**	**Not concerned**
Using web browsers	1	10
Using communication platforms (e.g., social networks, chatrooms, or email)	4	7
Playing multiplayer games	3	8
Using file-sharing platforms	3	8
Making an app purchase	2	9
Accessing inappropriate content	5	6
Accepting people as friends without knowing them offline	4	7
Inappropriate chatting with people	4	7
Sharing personal information with unknown people	4	7
Using a camera/microphone with unknown people	3	8
Downloading inappropriate application	5	6
Spending too much time on the Internet	4	7

6.2.1.5 Participants' mediation of their children's Internet use

Most of the participants reported using active and restrictive mediation and technical mediation, and half the parents monitored their children's Internet use, as shown in Table 31. Parents with varying levels of concern also used different parental mediation to manage their children's Internet use, as shown in Table 32. The majority of parents who were not concerned about their children's Internet use employed active mediation to discuss Internet safety with their children and guide them. More than half the parents who did not consider themselves to be concerned were already monitoring their children's Internet use afterwards and used technical mediation. In comparison, the majority of parents who were concerned about their children's Internet use used restrictive mediation to limit their children's Internet use, active mediation and technical mediation.

Table 31: Parental mediation used by participants

Parental mediation used	**Parents (no.)**	**Parents (%)**
Active mediation	21	70
Restrictive mediation	19	63
Monitoring	16	53
Technical mediation	18	60
None	1	3

Table 32: Parental mediations used by participants with different concern levels

	Parents' level of concern		
Parental mediation used	**Not concerned (11)**	**Somewhat concerned (17)**	**Very concerned (2)**
Active mediation	8	11	2
Restrictive mediation	5	14	0
Monitoring	6	8	2
Technical mediation	6	10	2
None	1	0	0

Parents differed in their concerns about their children's Internet use at different ages. The results regarding parents' use of parental mediation with their children at different ages are presented in Table 33. Most of the parents of young children were concerned about their children's Internet use, and nearly all of them had used active mediation to guide their children's Internet use and restrictive mediation. In addition, more than half the parents of younger children had used technical mediation. In comparison, half the parents of older children were concerned and the other half were not. Most of the parents who were not concerned about their older children had used active mediation to guide their children in using the Internet safely, and half used restrictive mediation to set rules that restricted their children's use, as well as monitoring. Nearly all the parents who were concerned about their older children used restrictive mediation, technical mediation, and monitoring. Generally, parents who were not concerned used active mediation and parents who were concerned used most mediation types with their children: active, restrictive, and technical.

Table 33: Parental mediation used with children in different age groups

		Parents' level of concern								
		Not concerned (11)			Somewhat concerned (17)			Very concerned (2)		
	Children's age	**4-7 (2)**	**8-11 (2)**	**12-16 (7)**	**4-7 (9)**	**8-11 (2)**	**12-16 (6)**	**4-7 (1)**	**8-11**	**12-16 (1)**
Parental mediation used	Active mediation	2	1	5	8	1	2	1		1
	Restrictive mediation	-	1	4	8	1	5	-		-
	Monitoring	1	1	4	3	1	4	1		1
	Technical mediation	1	2	3	5	-	5	1		1
	None	-	-	1	-	-	-	-		-

6.2.1.6 Participants' use of technical parental controls

Most of the participants used the parental controls built into the device operating system, such as BT, Android, iPhone, and Windows parental controls. Some of the parents used the parental control provided by the service provider (EE). Results relating to parents' use of parental control functions and satisfaction levels are presented in Table 34. Most of the parents used parental controls to restrict their children's Internet use and were satisfied with the functions provided.

Table 34: Participants' use of existing parental controls

Existing parental control usage		**No. of parents**
Features used	Monitoring the child's online activities.	5
	Restricting the child's online activities.	16
Satisfaction level	Very Satisfied	1
	Satisfied	10
	Neutral	5
	Dissatisfied	1
	Very Dissatisfied	0
Total of parents who used technical mediation		17

6.2.2 Participants' attitudes and performance with the system

The majority of the parents were satisfied with the system and they found the system was clear, simple, and easy to use. Some parents thought that time was needed to get used to all the system's functions. Parents also liked the options and functions provided by the system for managing settings for each child individually (assigning general protection responses for different risk events and managing each risky activity and customizing the protection responses), some parents also prefer to have a link to advice about parental mediation and the risk associated with a specific activity to help them to assess activity risk level. In addition, parents were satisfied with the protection response options, such as disallowing a child's activity, and contacting the child to discuss the activity with their children and to know why it had happened and advise them. On the other hand, some parents preferred avoiding contacting the child and having the system issue awareness raising to give him/her an opportunity to learn and understand the risk. Parents could, therefore, assign different responses depending on their perspective. Parents also liked the notification provided by system that provides them with more details when the child has tried to do something that is high/medium risk as parents might be unaware of what the child actually does, the warning presented for the child about the consequences of his/her activities, and the additional protection options.

Furthermore, the results of usability evaluation of the system was satisfied. After analysis of the video recordings of the experiment, most of the parents managed to use the system and complete the tasks (23 participants have completed the first task, 20 have completed the second task), as shown in Table 35.

Table 35: Participants' completion of tasks 1 and 2

Participant	Task 1		Task 2	
	Done without assistance	Done with assistance	Done without assistance	Done with assistance
P #1	✓			✓
P #2	✓		✓	
P #3		✓	×	
P #4	✓			✓
P #5	✓		✓	
P #6		✓	~	
P #7		✓	✓	
P #8	✓		✓	
P #9	~			~
P #10	✓			~
P #11	✓		✓	
P #12	✓		✓	
P #13	✓		~	
P #14	~		✓	
P #15		✓	~	
P #16	✓			✓
P #17	✓			~
P #18		~		✓
P #19	~		✓	
P #20	✓		✓	
P #21	✓		✓	
P #22	✓		~	
P #23		✓		✓
P #24	✓		~	
P #25	✓		✓	
P #26	✓		✓	
P #27	~			~
P #28	✓		✓	
P #29	✓		~	
P #30		~	~	
Total	23	7	20	9

~ = Done with some navigation problems

The participants' performance of the two tasks could have been influenced by the parents' concerns and experiences of using existing parental controls. The first task was to assign general protection responses for different risk events (low, medium, and high) and the second task was to assess the risk level of a specific activity and customise the protection responses. Thus, parents' performances in each task could differ depending on their attitudes and concern levels (i.e., if they preferred to assign a general protection response or to manage each activity individually) and their experience of using parental control tools, as shown in Table 36. So, the system could serve parents with different concerns.

In relation to the first task, some parents were concerned about specific activities, so, they prefer to check the risk levels and assign protection responses to specific activities rather than assign general protection responses in this task. Thus, the assistance in this task was explaining the facility provided by the system to assign general protection responses to any activity that would put a child at a low, medium, or high risk level.

In relation to the second task, some parents were not concerned about specific activities and might not have been interested in assessing each activity individually for this task, so, they prefer to assign general protection response rather than managing each activity individually. Thus, the assistance given for the task involved explaining the facility provided by the system to assessing the risk level of each activity and customising the protection response. In addition, the use of existing technical parental controls could have affected the parents' performance of the task. Some people had learned a particular way of managing their children's Internet use, such as putting a restriction (blocking) on the child's Internet use, without assessing the risk levels of the activities and were only able to work in that way, whereas other people could understand the new principle and adapt it to suit different contexts. Thus, some of the parents expected to work in the same way and thought the activities risk levels were already classified, so simply assigned the general protection responses. In comparison, parents who did not use parental controls felt confused about using the system and tried to change the response to the web activities that had been undertaken by the child in the last 24 hours. So, assistance was given in explaining the system options that enabled parents to assess the risk level of an activity and assign a protection response if the child tried to access the same content later.

Overall, the parents' performance can be classified into three groups, depending on their concerns and use of existing parental controls:

A. Parents who were not concerned

The majority of the parents who were not concerned completed the first task without assistance. One parent who was not generally concerned about her child's Internet use (1 out of 11) was, however, concerned about specific activities and wanted to check the risk levels of activities by seeing what the child had done in order to assign a protection response.

The number of parents who needed assistance increased for the second task: four parents (4 out of 11) needed assistance to assess each activity and customise the protection response. They might not, however, have been concerned about specific online activities and might not be interested in assessing each activity individually. Three of the parents were familiar with the restriction setting in existing parental controls without assessing the activities risk levels and they might have expected to work in the same way; the other parent did not have experience of using parental controls as he reported: *"I have trouble with technology and have not thought about using these applications"*. Thus, they thought that the risk levels of the activities had already been classified and tried to assign general protection responses.

B. Parents who were somewhat concerned

The majority of the parents who were concerned completed the first task without assistance. However, five of the parents who were somewhat concerned about their children's online activities (5 out of 17) needed assistance to assign a general protection response during the first task. Four parents were worried about specific activities which had already been done by their children, so they and tried to assign protection responses for these activities individually; and one parent might not have enough experience and knowledge of children's online activities as her child was young (aged 4-7) and a less frequent user, so, she wanted to check what the child had done to see the risk levels of the activities before assigning the protection responses.

During the second task, four parents (4 out of 17) needed assistance to assess each activity and customise the protection response. Two of the parents did not have experience in using parental controls and were confused about using the system, such as changing the response taken to the web activities that had been done by the child. The other two parents were familiar with the restriction setting in existing parental controls without assessing the activities risk levels and might have expected to work in the same way. They assumed that the activities risk levels had already been classified and tried to assign general protection responses.

C. Parents who were very concerned

This group had just two participants, which is not enough to distinguish the participants' performance of different tasks. One parent who was very concerned about his child's online activities (1 out of 2) needed assistance to assign a general protection response during the first task. He might not have enough experience and knowledge of children's online activities as his child was young (aged 4-7) and a less frequent user, so, he tried to check what the child had done to see the activities risk levels in order to assign a protection response.

Both parents also needed assistance in the second task to assess each activity and customise the protection response. They were familiar with restriction settings provided by existing parental controls without assessing activities risk level and they might have expected to work in the same way. They expected the activities risk levels to already have been classified and tried to assign general protection responses.

In addition, some parents encountered difficulties in using the system to find the required options such as assigning a general protection response option and assessing activity risk level option (i.e., navigation problems). They were confused about the monitoring options, and clicked the "Alert and report setting" option, and the "View activities reports in different application categories" option.

Table 36: Parents' performance of tasks 1 and 2

Parental concern level	Existing technical parental controls	Task	Participants who needed assistance	Participants who did not need assistance	Participants who need assistance	
					Participant's action (misunderstanding, error)	**Potential reason for needing assistance**
Not concerned	Parental control used	T 1	1	5	Checking what the child has done in order to assign a protection response based on this activity.	No concern generally but some concern about specific activities.
		T 2	3	3	Assigning general protection responses as they expect the activities risk levels are already classified.	No concern about specific activities, as well as familiarity with the restriction setting in existing parental controls without assessing activities risk level and expectation of working in the same way (inability to adapt and understand a new context).
	No parental control used	T 1	-	5	-	-
		T 2	1	4	Assigning general protection responses and expecting the activities risk levels to already be classified.	No concern about specific activities and no experience in using parental control applications.
Somewhat concerned	Parental control used	T 1	5	5	Assigning protection responses for specific activities individually.	Concern about specific activities.
					Checking what the child has done in order to assign a protection response based on this activity.	Concern about specific activities, and less experience (the child is a less frequent user).

		T 2	2	8	Assigning general protection responses and expecting the activities risk levels to already be classified.	Familiarity with restriction settings in existing parental controls without assessing activities risk level and expectation of working in the same way (inability to adapt and understand a new context), and less experience (the child is a less frequent user).
	No parental control used	T 1	-	7	-	-
		T 2	2	5	Confused about using the system and changing the response taken for the web activities that have been done by child.	No experience in using parental control applications.
Very concerned	Parental control used	T 1	1	1	Checking what the child has done in order to assign a protection response based on this activity.	Concern about specific activities, and less experience (the child is a less frequent user).
		T 2	2	-	Assigning general protection responses and expecting the activities risk levels to already be classified.	Familiarity with restriction settings in existing parental controls without assessing activities risk level and expectation of working in the same way (inability to adapt and understand a new context), and less experience (the child is a less frequent user).
	No parental control used	T 1				
		T 2				

6.2.3 Task completion times

The time taken for tasks to be completed was measured. The average time for the whole experiment was 43 minutes. The time taken to perform the first task was 3 minutes, whereas the time required to perform the second task was 6 minutes. The second task took longer as it requires more steps. The time taken for task completions is displayed in Table 37. There is a difference in the time taken for tasks to be completed between participants who performed the tasks with/without assistance. The mean time was approximately 3 minutes for the first task and 5 minutes for the second task for participants who completed it without assistance; the mean was approximately 5 minutes for the first task and 8 minutes for the second task for participants who completed the task with assistance. This difference could be interpreted as reflecting differences in the participants' concerns, as well as their experience of using parental controls.

Table 37: Time taken for tasks to be completed

Participant	**Time spent on task 1**		**Time spent on task 2**	
	Participants who completed without assistance	**Participants who completed with assistance**	**Participants who completed without assistance**	**Participants who completed with assistance**
P #1	2	-	-	13
P #2	5	-	17	-
P #3	-	3	×	
P #4	1	-	-	6
P #5	2	-	5	-
P #6	-	3	4	-
P #7	-	3	2	-
P #8	2	-	3	-
P #9	3	-	-	5
P #10	2	-	-	9
P #11	2	-	6	-
P #12	3	-	3	-
P #13	3	-	3	-
P #14	3	-	4	-
P #15	-	5	10	-
P #16	8	-	-	11
P #17	3	-	-	5

P #18	-	5	-	9
P #19	3	-	4	-
P #20	3	-	4	-
P #21	2	-	3	-
P #22	3	-	6	-
P #23	-	9	-	8
P #24	1	-	6	-
P #25	2	-	4	-
P #26	2	-	6	-
P #27	4	-	-	4
P #28	2	-	5	-
P #29	2	-	7	-
P #30	-	7	3	-
Total	63	35	105	70
Average	$2.7 \simeq 3$	5	5	$7.7 \simeq 8$

6.2.4 Parents' level of satisfaction with the system

This subsection discusses the participants' level of satisfaction with the system. Participants were asked to rate their satisfaction level towards the system at the end of the experiment. The post-survey elicited feedback about the participants' understanding of the system concept, and satisfaction with the system design and functions, and their preferences to improve the system's effectiveness towards the system.

6.2.3.1 Parents' understanding of the system concept

Participants were required to grade their understanding of the system concept (calculating and predicting the risk levels of children's online activities in order to warn parents and protect children online), as displayed in Figure 37. The majority of the participants (96%) felt that the concept of the system was very clear or clear and that it would enable parents to assess the risk levels of children's online activities and assign appropriate protection responses.

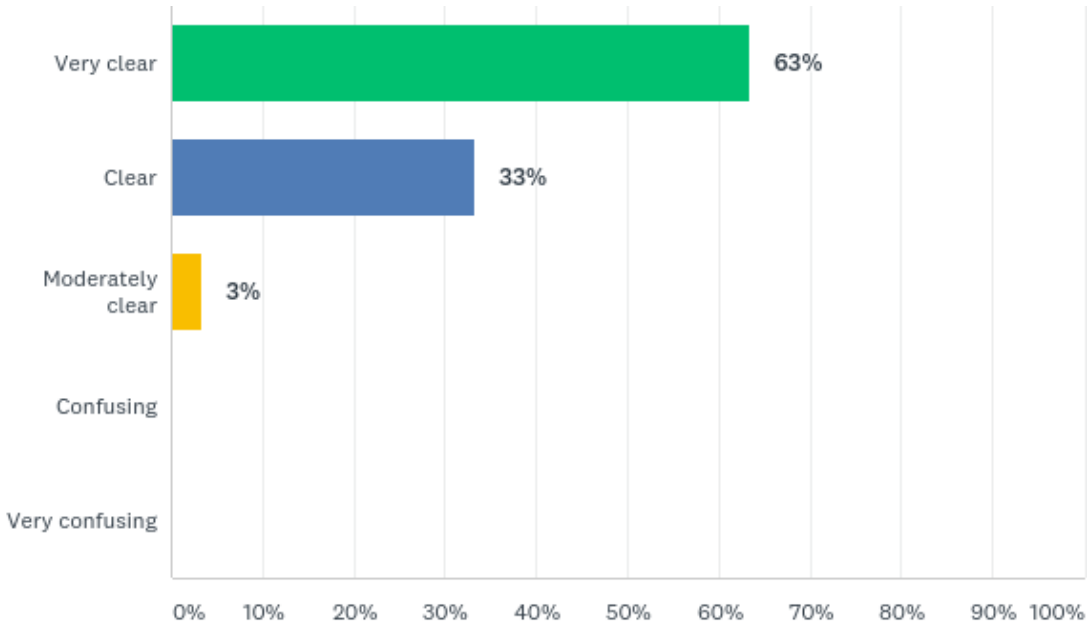


Figure 37: Participants' responses regarding the clarity of the system concept

6.2.3.2 Parents' satisfaction with the system design and functions

The participants were asked to indicate their agreement with a number of statements about the system design and functionalities, as displayed in Figure 38 and Table 38 below. It is clear from the table that the level of participants' satisfaction was high in terms of the overall appearance of the system; they found the amount of information was appropriate and sufficient; the concepts and terms were clear; the functions provided by the system were clear and appropriate (i.e., assigning general protection responses for different risk events, and assessing the risk level of an activity and customising appropriate protection responses); the alert was understandable and informative; and they found the system easy to use. Although some of the participants needed assistance, they all agreed that the system was meaningful and useful.

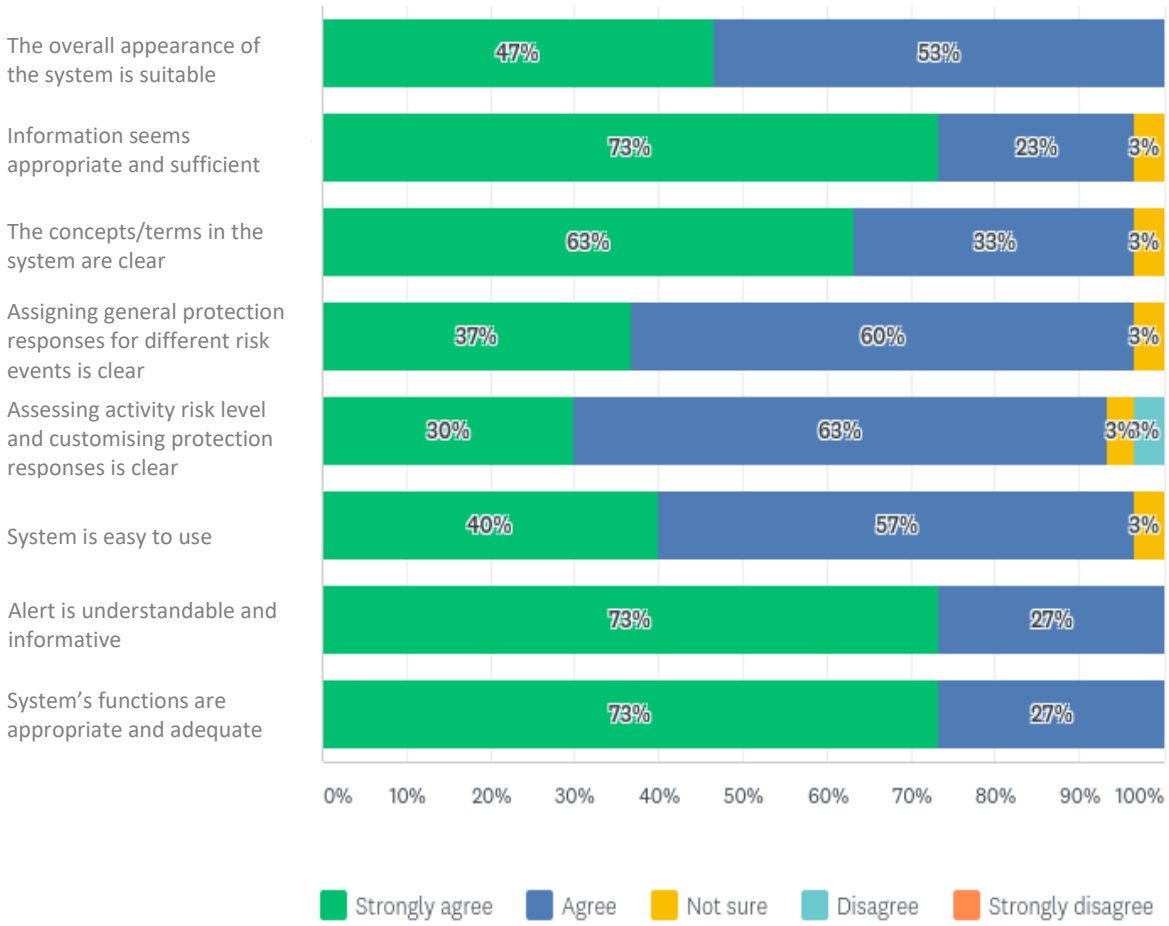


Figure 38: Participants' satisfaction with the system design and functionalities

Table 38: Participants' satisfaction with the system design and functionalities

System usability and usefulness	Participants' responses					Total
	Strongly agree	Agree	Not sure	Disagree	Strongly disagree	
The overall appearance of the system is suitable.	14	16	0	0	0	30
The amount of information seems appropriate and sufficient.	22	7	1	0	0	30
The concepts/terms in the system are clear.	19	10	1	0	0	30
It's clear how to assign general protection responses for different risk events (low, medium, and high).	11	18	1	0	0	30
It's clear how to assess the risk level of an activity and customise specific appropriate protection responses.	9	19	1	1	0	30
Overall, the system is easy to use.	12	17	1	0	0	30
The issued alert is understandable and informative.	22	8	0	0	0	30
The functions provided by system are appropriate and adequate.	22	8	0	0	0	30

Overall, the majority of the parents prefer to use the system to manage their children's Internet use, only two parents of older children did not find the system to be necessary in their case as they treated their children as young adults (they stated: "*Because my son is now going into 6th form. If I had younger children then I would consider using this system"; "not necessary for my child [16]*").

Also, the parents reported their thoughts about their experience and preferences. Participants' comments about what they liked and functions that could be added to improve the system's effectiveness are presented in Table 39. They found the system to be clear, easy to use, and provided a comprehensive range of options and functions to manage and protect their children's Internet use. They also liked the notification providing the parent with more details about the child's activity. Some parents provides some suggestions related to the system design (such as

preferring a colourful interface with larger buttons; the suggestion to have a top-level overview screen to manage the responses for high, medium, and low risk and provide explanations of the terminology). Some parents also prefer to have a link to advice about parental mediation and the risk associated with a specific activity, and managing each application individually, such as Netflix. Some suggestions were related to the alert and response options, such as seeing the path of access to know if this had happened accidentally or intentionally, providing a snapshot of the blocked content on a website in the alert preferred to know if the inappropriate content was a text or video, and also providing an option for notifying the service provider about inappropriate content. Some parents suggested having a version of the proposed parental control system for game devices (e.g., Xbox) and tracking the child's location feature. These suggestions can be considered and perhaps added to the fully functional system. Additional features were suggested that seemed to be beyond the scope of the system, such as providing different application ratings for different countries, although this actually depends on the app store; for example, Apple App Store ratings and rankings are country-specific (i.e., there are differences between App Stores depending on the country). However, parents could use the system to monitor and manage the downloading of inappropriate applications.

Table 39: Participants' comments about the system

Comments			**Participant**
Preferred aspects	1	*"I would definitely use this system, it is good protection when my child is using the Internet. I think it seems to have everything in place already."*	P #1
	2	*"It seems fairly common sense."*	P #2
	3	*"Like the way it can be customised for different aged children."*	P #3
	4	*"As much as I monitor my child's Internet use, this would provide further protection."*	P #4
	5	*"Although not finished, the app could be clearer and a little more user friendly in appearance. I did like the function and idea of what it can perform. The look overall was a little basic but I do like the idea behind it and would use it at home with my child."*	P #5
	6	*"I think that this is a useful tool to have - the child would be aware that the parent has access - it is also better than having to 'keep on checking' - the child would know the consequences of going over the boundaries but also will protect the innocence of the child using the Internet."*	P #8
	7	*"I do like the new system, it would work rather well in today's moving day."*	P #10
	8	*"I'm aware that some apps appear harmless but are actually high risk and many parents are unaware of what they actually do. This system is really helpful in alerting parents to the type of content that their children are using."*	P #12
	9	*"I would use the system when my child is older and spends time on the Internet alone."*	P #13
	10	*"Individual settings for each child is good."*	P #15
	11	*"The system provides a clear, simple and yet comprehensive range of options to enable the parent to control access to or not access to web browser, inappropriate content and usage times. I particularly like the facility whereby the system alerts you to the attempt to access inappropriate content and enable you to then contact the child in real time in order to advise and discuss with the child after being given advice and guidance by the system yourself.* *I find the app clear and comprehensive, with the right blend of enabling/disabling controls, provision of ability to contact and advise the child, and, if need be, put sanctions and/or limits in place, temporary or otherwise."*	P #19
	12	*"I am very impressed with this application. I think it seems easy to use and understand what you are restricting, I like that it notifies you when your child has tried to do something deemed as high/medium risk."*	P #21
	13	*"Very good and well thought out."*	P #22
	14	*"It is very useful and can be more specific in some parts."*	P #24
	15	*"Using this system would make me feel much happier about allowing my children access to the Internet."*	P #25
	16	*"I think it is a really good system, easy to navigate and very well thought out. Something I would definitely use."*	P #28
	17	*"The system provides good protection notification for both parent and child. The system is clear and appears effective."*	P #30

Suggestions related to system design	1	*"Although it is clear I would need some time to get used to all the functions."*	P #1
	2	*"Explanations of the terminology."*	P #3
	3	*"Bigger buttons and clearer signposting to set restrictions easily."*	P #5
	4	*"Perhaps the design could be more colourful."*	P #20
	5	*"I would just like a nice bright top-level overview screen with minimal data high is on, medium is on, low is on and if I want to adjust those settings, I just click on the word to drill down. Just clarity and speed of set up. That's it a great app."*	P #22
	6	*"The menu for assessing the level of risk for particular situations was hard to find. I would use this system, but when my children were a bit older I expect."*	P #29
Suggestions related to system functions	1	*"To notify the web browser of inappropriate content accessed by a child."*	P #4
	2	*"Maybe it is effective to have an option to use other countries' categories of age restrictions. Track the location."*	P #6
	3	*"Snapshot of website to parent, a maliciousness warning."*	P #10
	4	*"I like the concept of this, I wonder how it would work with devices such as gaming systems (e.g., Xbox) I can see how it would work with a smartphone or tablet. How do you make sure the child can't change the settings/override it!"*	P #11
	5	*"Maybe a link to some information or a website giving advice on parental mediation, health risks associated with long amounts of time spent online and so on."*	P #12
	6	*"I think it would be useful to have the application rate content of other applications such as Netflix. This would allow the child to use the app but restrict it to only suitable content within the application.* *"Keep a log of all Internet activity regardless of risk."*	P #14

6.3 Discussion

The majority of the parents who took part in the experiment were satisfied with the system in terms of its overall appearance and the functions provided. The majority of the parents managed to perform the tasks successfully, that proved the system is simple and easy to use. Some participants encountered difficulties while performing their assigned tasks, although these difficulties could be addressed through improve the system design. The difficulties and errors can be classified into two categories. The first category could be related to the system design and navigation. System navigation can affect user interaction with a system and, consequently, the performance of tasks. Some participants were confused about the monitoring options displayed in the main interface of the child's account due to options related to monitoring the child's activities, such as the "Alert and report setting" and the "View activities reports in different application categories" options. Some of the parents became confused and tried to change the response to previous activities conducted by the child and found it hard to find the options for managing protection responses. Thus, it is worth considering simplifying the interface and reducing the options for monitoring that are displayed in the main interface. Instead, the main interface could display one option for monitoring a child's activities, which could lead to further monitoring options.

The second category of errors and difficulties is related to system function organisation. Some of the parents experienced difficulties in performing the tasks independently. For example, some parents wanted to check/assess the risk level of activities before assigning general protection responses. On the other hand, some parents thought that the activities risk levels were already classified when they assigned the general protection responses. Therefore, based on the observed confusion, an alternative way of visualising the system functions (see Figure 39) would be for the system to display the general protection responses and activities risk levels in the same interface in order to show the information more clearly. Parents could then check the

protection responses that would be taken with different risk levels and change them if they wished.

Figure 39: System interfaces after changes in response to parents' feedback

In general, parents were satisfied and liked the new proposed parental control tool. The existing parental controls focus on monitoring children's Internet use, and blocking that use, so, parents find them are restrictive and have difficulty in working with them (e.g., changing the parental control settings). Furthermore, some parents are unaware of their children's online activities and Internet risks (As mentioned previously in section 2.4). Thus, the proposed parental control system aimed to address these issues through providing a simple, flexible and adaptable parental control tool that use risk assessment and communication mechanism for managing children's online activities and raising awareness about the potential risks for parents and help them make informed decisions. Online risk incidents occurrences and its resulted harm could be connected to the individual factor of child (e.g., child's age, child's experience and psychological characteristics) and also the methods that child used to access and use the Internet (e.g., device type, access location). So, the proposed system consider the factors that could increase exposure to online risks and assesses the potential risk of online activities, and then raises awareness about these risks for parents in a continuous manner. So, parents could know what their children do online and the associated risks, and thus they can identify the level of control suitable for their children's needs.

Furthermore, the findings shows that parents were satisfied with the system concept (calculating and predicting the risk levels of children's online activities and raising awareness about these risks). Parents were able to use and understand the system and liked the flexibility and facilities provided by the system for managing children's online activities individually and customizing protection responses for these activities. Also, parents liked the immediate alert that gave them useful information and warned them about what the child had attempted to do, as well as provided additional protection options to protect the child. So, applying risk communication mechanisms to parental controls helps parents understand the potential risks to which children may be exposed before the danger is actually realised. The proposed system provides a flexible

and adaptable parental control that enables parents to be engaged in the risk assessment process and gives them a granular level of control over their children's online activities.

Chapter 7: Conclusions and future work

Children and young people start using new technologies early as a source of information, education and entertainment. There is, however, no doubt that new technologies expose young people to a wide range of risks. Therefore, there is a need to safeguard young people online and raise security awareness in order for them to acknowledge the opportunities and avoid online risks.

The main objective of this research was to provide a flexible and adaptable form of parental control that would enable the provision of real-time interventions to raise risk awareness for both parents, so that they have a chance to understand potential risk before the danger is realised. This objective was achieved by first presenting a comprehensive review of the literature on the existing methods of safeguarding children online, which included the information security awareness initiatives for children and the parental control software currently available. The research then reviewed the risk assessment and communication approaches used to raise security awareness about specific security issues in real time. This enabled a risk communication framework for parental control to be designed and a prototype system implemented. Finally, the prototype system was evaluated by parents to assess its usability and usefulness.

This chapter concludes the thesis by highlighting the principal achievements of the research and discussing its limitations. It also presents suggestions for potential future improvement of the proposed system.

7.1 Achievements of the research

The research has met all the objectives specified in Chapter 1. The objectives and specific achievements were as follows.

- Objective 1: Investigated children's online children's online practices and experiences. The advance of mobile devices has expanded children's Internet use by providing 'anywhere, anytime' accessibility. Thus, the continuing rise in Internet use by young people has increased the online risks and harm. Also, there are some factors could increase exposure to online risk such as the individual factors of child (child's age, psychological characteristics), and factors related to child's internet access and use (device type, access location, time spent online and frequency of use). Furthermore, young people are not always cautious, they engaged in risky online activities without being aware of the consequent threat. In addition, some parents are unaware of their children's online activities and Internet risks. Also, a minority of parents use parental control software, and some parents find parental control software are too restrictive. So, the security mechanism should be flexible and take into account the factors that increase the probability of child's exposure to online risks in order to predict the potential risks and raise awareness about these risks before the danger is actually realised and help parents to take the conscious decision.
- Objective 2: Reviewed the current methods for safeguarding young people, which involve the investigation of existing information security awareness initiatives and parental control software available for parents. The current parental control methods help parents to monitor children's Internet use and restrict that use, but do not assess the risk of children online activities and raise awareness about these potential risks to help parents make the right decisions. Also, information security awareness initiatives present advice and different resources for raising awareness about Internet safety in separate websites. So, none has made parents and children aware of the potential risks and the implications associated with children online activities in real time and means of safeguarding against them. Thus, the review highlighted Internet safety awareness initiatives should be integrated with parental controls. So, parental controls should be able to predict and assess the potential risk involved

in children online activities and raise awareness about these risks in a continuous manner. Thus, parents could know what their children do online and the associated risks, and thus they can identify the level of control suitable for their children's use. To this end, risk communication technology could be used in parental control to assess risks associated with children's online activities and raise awareness about the potential risks and help parents and young people understand the potential risks and make good security decisions.

- Objective 3: Proposed a risk communication framework for parental control that to raise awareness of potential risks for parents and give them a granular level of control to manage their child(ren)'s Internet use. The system framework monitors children's online activities, assesses the risk levels of children's online activities, and issues the protection responses based on the resulted risk level. A risk assessment model was also proposed that calculates the risk level of children's online activities based on likelihood and impact (severity of harm). The likelihood is evaluated based on children risky online activities and factors that could increase the probability of harm such as child's age, experience, psychological characters, and other factors related to child's Internet access and use.
- Objective 4: Developed and implemented a proof of concept of the proposed framework to gain insight into its functionalities. A prototype simulates the proposed system and provides a clear image of its functionalities and how it is intended to work. The prototype system described the system's interfaces and detailed the process of the risk assessment of children's online activities and customisation of protection responses.
- Objective 5: Evaluated the usability and usefulness of the proposed system among a group of parents. After implementing the prototype system, the prototype system is evaluated to gain parents' feedback about the system. The evaluation approach involved asking parents to use the prototype system and perform certain tasks (i.e., assessing the context of a child's Internet use and customising the protection response to the context), that helped to identify the participants' impressions about the system and potential usage difficulties. Also, the

experiment involved pre-test questionnaire to gain insight into children' online experiences and parents' concerns and use of parental mediation which was useful for the interpretation of the parents' interaction during the experiment. In addition, a post-test evaluation questionnaire was used to gain feedback about parents' satisfactions about the system.

- Objective 6: Analysed the data collected from the evaluation experiment. The findings provided indication about participants' satisfactions with the system. The majority of the participants were satisfied with the new proposed parental control tool in terms of its overall appearance and the functions provided. They managed to perform the tasks successfully, that proved the system is simple and easy to use. Also, parents liked the flexibility and facilities provided by the system for managing children's online activities individually and customizing protection responses for these activities. Thus, the proposed system provides a simple, flexible and adaptable parental control tool for managing children's online activities.

7.2 Limitations of the research

Despite the achievement of the overall objectives of the research programme outlined in the previous section, there are some limitations associated with the work. The main limitations of the research are listed below.

- The implementation of the fully functional system in a real environment was challenging, due to the requirement for the system concept to be assessed first by parents to establish whether the system is useful, usable, acceptable and satisfactory. Then, the system could be implemented and used in a real environment and the child-parent interaction with the system evaluated. A full implementation of the system would be very useful to evaluate this approach in a real-world environment, as this would offer better understanding of its effectiveness. Considering the nature of the research, the implementation and evaluation of the fully functional system is difficult due to the research programme being limited by a

certain time frame. The time available for the research did not permit full implementation of the system.

- The system's usability and usefulness were assessed by 30 parents using prototype software that simulated the main functions of the system (i.e., assessing the risk levels of activities and assigning protection responses). The experiment results show that the majority of the parents were satisfied with the system in terms of its overall appearance and the functions provided, and they were able to perform the tasks successfully. Although the population was not big enough to classify the participants' performance with the system and identify potential reasons for those participants needing assistance to perform the tasks, the experiment results gave an indication that parents' concerns and experiences of using existing parental controls could have influenced their interactions with the proposed system. It was difficult to conduct the experiment with a wide range of participants, as the research employed a mixed evaluation approach and treating a large sample would have been costly and time consuming.
- A default setting for the risk assessment model was not tested and evaluated across different children in a real environment. A more accurate calculation of the values of the factors involved in the risk assessment model would need to be based upon real incidents. Unfortunately, the research process lacked sufficient resources to report real incidents of children's exposure to online risks precisely with more details about the effect of the factors included in the risk assessment model. Thus, the trial and practical use of the model in a real environment with further analysis could provide insights into the effectiveness of the model and the more accurate values that could be considered in the system. Further monitoring and analysis of children's Internet use might also detect further factors that could contribute to the occurrence of risk.
- A default setting for appropriate responses to different activities is proposed. Protection responses could differ according to a child's age and behaviour. Protection responses could

be refined over time using the system, and the most suitable responses to each activity for children in different age groups could be considered by the system.

7.3 Suggestions and scope for future work

The main achievements and limitations of the research were stated in the previous sections. However, there are several opportunities for further investigations and improvements to be carried out in future research. These suggestions are outlined below.

- A complete version of the system needs to be developed and implemented in a real environment. This would be beneficial in order to understand the effectiveness of the system in protecting children online and raising awareness for parents and children about potential risks. Parents and children could then understand the implications of online activities and make the right choices and children could use the Internet safely. Evaluating a fully functional system working in a live environment with a wide range of participants would also provide a richer and more comprehensive set of participants' (parents' and children's) perspectives and interactions with the system and facilitate the identification of limitations.
- The risk assessment model could be refined over time using the system in a real environment. The practical use of the system in a real environment could, with further analysis, provide insight into the effectiveness of the model and more accurate values that could be considered in the system.
- A default set of responses could also be refined over time using the system with a wide range of children of different ages. The most suitable responses to each activity could be refined by the system based on the reactions of children in different age groups and their online behaviour. Parents could also provide feedback about the efficiency of the responses issued for protecting their children, such as whether the responses were successful and appropriate, and whether they had unwanted side effects for the child. Thus, machine

learning algorithms could also be integrated into the system in order to improve its learning ability and appropriate responses could be automatically determined.

- With full system implementation, awareness raising for children should be presented in a simple and understandable way for each activity according to the children's age and their cognitive abilities.

7.4 Importance of protecting children online

The Internet has become a primary foundation in children's lives for the acquisition of knowledge, as well as entertainment. In addition, the continuing rise in the use of alternative portable devices, such as smartphones and tablets, has increased children's online activity, with a corresponding rise in online risks. Furthermore, young people are not always cautious when they use the Internet, and they involved in harmful online activities without being aware of the implications of these activities (Annansingh and Veli 2016)(Sithira and Nguwi 2014). Furthermore, some young people are also unaware of how safeguarding their online behaviour such as changing privacy setting (Ofcom 2020). Also, some parents have a low level of awareness of Internet risks and their children's online activities (Symons et al. 2016). In addition, some parents find difficulties in control their child's screen time especially when children get older (Ofcom 2019b). Furthermore, a few parents use parental control applications for blocking, filtering and monitoring their children's Internet use (Anderson 2016) (Ofcom 2019b). Parents often have difficulty in working with parental control software (AV-Comparatives, 2014) (Pons-Salvador et al. 2018). Also, parents find parental controls are inadequate and restrictive (AV-Comparatives, 2014) (Ofcom 2019b).).

So, parental controls should be easy to use, flexible, and able to raise awareness about the potential risks of children's online activities for parents and children in order to help them to make informed decisions. Parents and children should be aware of Internet safety and the implications of online activities, and how to cope with the risks and harm they encounter. Integrating security awareness with parental controls may be an effective solution to help

parents and protecting young people online. Thus, the main objective of the proposed framework was to use a risk communication approach to raise awareness of the risks associated with children's online activities and enable them to make good security decisions. Risk communication technologies could help safeguard young people online by identifying and calculating the risk level of each action and delivering warnings before the danger is actually realised, as well as providing appropriate mitigating actions in accordance with the resulted risk level.

There are two main reasons why the work proposed in this study is deemed necessary and worthwhile. Firstly, no studies have been known to address risk communication approaches to promote online safety for parents and young people. Secondly, while theoretical research has investigated factors affecting children's online experiences in relation to exposure to online risks, none has employed those factors in an integrated framework. From the perspective of the author, the proposed model can assess the risk level of online activities conducted by different children, in order to raise awareness of the potential risks for parents and children and help them make informed decisions.

References

A Common Sense Media Research Study. 2012. “Social Media, Social Life: How Teens View Their Digital Lives.”

ACMA (Australian Communications and Media Authority). 2008. “Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety.” *Communications and the Digital Economy*. http://docplayer.net/16378169-Developments-in-internet-filtering-technologies-and-other-measures-for-promoting-online-safety.html.

Anderson, Monica. 2016. “How Parents Monitor Their Teen’s Digital Behavior.” *Pew Research Center: Internet, Science & Tech* (blog). January 7, 2016. http://www.pewinternet.org/2016/01/07/how-parents-monitor-their-teens-digital-behavior/.

Annansingh, Fenio, and Thomas Veli. 2016. “An Investigation into Risks Awareness and E-Safety Needs of Children on the Internet: A Study of Devon, UK.” *Interactive Technology and Smart Education*, May. http://www.emeraldinsight.com/doi/abs/10.1108/ITSE-09-2015-0029.

Apple. 2020. “Use Screen Time on Your IPhone, IPad or IPod Touch.” 2020. https://support.apple.com/en-gb/HT201304.

Association, Press. 2014. “Number of Children Who Are Victims of Cyberbullying Doubles in a Year.” *The Guardian*, November 14, 2014, sec. Society. https://www.theguardian.com/society/2014/nov/14/35pc-children-teenagers-victims-cyberbullying-fears-grooming-tinder-snapchat.

AV-Comparatives. 2014. “Parental Control Software Test and Review.” www.av-comparatives.org.

Booker, Cara. 2014. “Young People & Social Media: One Hour per Day Is Enough – Understanding Society.” 2014. https://www.understandingsociety.ac.uk/2014/05/20/social-media-one-hour-per-day-is-enough-for-our-kids.

Brand, Jeffrey E., and Stewart Todhunter. 2016. “DIGITAL AUSTRALIA REPORT.”

Catshill Learning Partnerships, Education technology association, and Naace. 2017. “Pupils Online: National Survey of 19,000 UK Pupils Reveals New Trends in Children’s Internet Use.”

“Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business.” 2013. Federal Trade Commission. June 30, 2013. https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

DeMarco, Jeffrey Nicholas, Carly Cheevers, Julia Davidson, Stefan Bogaerts, Ugo Pace, Mary Aiken, Vincenzo Caretti, Adriano Schimmenti, and Antonia Bifulco. 2017. “DIGITAL DANGERS AND CYBER-VICTIMISATION: A STUDY OF EUROPEAN ADOLESCENT ONLINE RISKY BEHAVIOUR FOR SEXUAL EXPLOITATION.” 2017.

Drevin, Lynette, and Günther R. Drevin. 2013. “Engagement of Young People in Social Networks: Awareness and Security.” *International Journal of Computer, Electrical, Automation, Control and Information Engineering* 7.

Ellis, Cat. 2020. “The Best Free Parental Control Software 2020: Keep Your Kids Safe Online.” 2020. https://www.techradar.com/best/free-parental-control-software.

Fire, Michael, Roy Goldschmidt, and Yuval Elovici. 2014. “Online Social Networks: Threats and Solutions.” *IEEE Communications Surveys & Tutorials* 16 (4): 2019–36. https://doi.org/10.1109/COMST.2014.2321628.

Fryling, Meg, Jami Lynn Cotler, Jack Rivituso, Lauren Mathews, and Shauna Pratico. 2015. “Cyberbullying or Normal Game Play? Impact of Age, Gender, and Experience on Cyberbullying in Multi-Player Online Gaming Environments: Perceptions from One Gaming Forum.” *Journal of Information Systems Applied Research* 8 (1): 4.

Goodman, R., H. Meltzer, and V. Bailey. 1998. “The Strengths and Difficulties Questionnaire: A Pilot Study on the Validity of the Self-Report Version.” *European Child & Adolescent Psychiatry* 7 (3): 125–30. https://doi.org/10.1007/s007870050057.

Google Play Help. n.d. “Set up Parental Controls on Google Play - Google Play Help.” Accessed February 8, 2020. https://support.google.com/googleplay/answer/1075738?hl=en-GB.

GRANT, JUSTIN. 2008. “Inside the Minds of Teens Who Post Sexual Images of Themselves.” Abc News. 2008. https://abcnews.go.com/TheLaw/story?id=6029237&page=1.

Haddon, Leslie, and Jane Vincent. 2014. “European Children and Their Carers’ Understanding of Use, Risks and Safety Issues Relating to Convergent Mobile Media.” http://www.kidsenjongeren.nl/wp-content/uploads/2012/09/NCGM_QualitativeReport_D4.pdf.

Hall, Brian. 2016. “Best Parental-Control and Cell Phone-Monitoring Apps 2017.” Tom’s Guide. 2016. http://www.tomsguide.com/us/best-parental-control-apps,review-2258.html.

HANNAH. 2017. “NTERNET SAFETY: A MOTHER’S STORY OF HOW A PAEDOPHILE GROOMED HER 11-YEAR-OLD DAUGHTER ONLINE.” The Independent. 2017. https://www.independent.co.uk/life-style/health-and-families/internet-safety-day-hannah-h-mother-paedophile-online-grooming-11-year-old-daughter-facebook-webcam-a7560801.html.

Hartikainen, Heidi, Netta Iivari, and Marianne Kinnula. 2015. “Children and Web 2.0: What They Do, What We Fear, and What Is Done to Make Them Safe.” In *Nordic Contributions in IS Research*, edited by Harri Oinas-Kukkonen, Netta Iivari, Kari Kuutti, Anssi Öörni, and Mikko Rajanen, 30–43. Lecture Notes in Business Information Processing 223. Springer International Publishing. https://doi.org/10.1007/978-3-319-21783-3_3.

Ito, Mizuko, Sonja Baumer, Matteo Bittanti, danah boyd, Rachel Cody, Becky Herr-Stephenson, Heather A. Horst, et al. 2010. “Hanging Out, Messing Around, and Geeking Out.” MIT Press. 2010. https://mitpress.mit.edu/books/hanging-out-messing-around-and-geeking-out.

Jeong, Yongick, and Erin Coyle. 2014. “What Are You Worrying About on Facebook and Twitter? An Empirical Investigation of Young Social Network Site Users’ Privacy Perceptions and Behaviors.” *Journal of Interactive Advertising* 14 (2): 51–59. https://doi.org/10.1080/15252019.2014.930678.

Johnston, Nicole. 2019. “Best Cell Phone Parental Control Software of 2019.” 2019. https://www.toptenreviews.com/best-cell-phone-parental-control-software.

Kang, Jina, Hyoungshick Kim, Yun Gyung Cheong, and Jun Ho Huh. 2015. “Visualizing Privacy Risks of Mobile Applications through a Privacy Meter.” In *Information Security Practice and Experience*, edited by Javier Lopez and Yongdong Wu, 9065:548–58. Cham: Springer International Publishing. http://link.springer.com/10.1007/978-3-319-17533-1_37.

Karabacak, Bilge, and Ibrahim Sogukpinar. 2005. “ISRAM: Information Security Risk Analysis Method.” *Computers & Security* 24 (2): 147–59. https://doi.org/10.1016/j.cose.2004.07.004.

Kaspersky Safe Kids. n.d. “Designed to Help You Protect Your Kids Online and Beyond.” https://me-en.kaspersky.com/safe-kids?redef=1&THRU&reseller=me-en_evrgrn_acq_ona_sem_bra_onl_b2c__psrch_____&ksid=ab4b0bf0-fb1f-48b1-81d5-f1aeda9d016d&ksprof_id=444&ksaffcode=704562&ksdevice=c&kschadid=303638288116&kschname=google&kpid=Google|1599371442|59360243446|303638288116|kwd-298323932875|c&gclid=CjwKCAiA35rxBRAWEiwADqB37_rmuFX56UU-UShHP1kjEMp6pOvbhLAN-_czmx2PdQtwPBYg-ug0yhoC3D0QAvD_BwE.

“Kidnapped by a Paedophile I Met Online.” 2016. BBC NEWS. 2016. https://www.bbc.co.uk/news/magazine-35730298.

“Kids Spend More Than 3 Hours a Day on Apps.” 2014. 2014. http://www.prnewswire.com/news-releases/kids-spend-more-than-3-hours-a-day-on-apps-275993041.html.

Kirik, Ali, Ahmet Arslan, Ahmet Çetinkaya, and Mehmet Gül. 2015. “A Quantitative Research on the Level of Social Media Addiction among Young People in Turkey.” *International Journal of Science Culture and Sport* 3 (October). https://doi.org/10.14486/IntJSCS444_.

Kongkarn, V., and S. Sukree. 2012. “A Framework for Applying an Intelligent Agent to Monitor, Interpret, and Report Risk of Online Computer Game Addiction in Children and Early Adolescents in Thailand.” In *Proceedings of 2012 IEEE-EMBS International Conference on Biomedical and Health Informatics*, 372–75. https://doi.org/10.1109/BHI.2012.6211592.

Koyuncu, Tugce, Alaettin Unsal, and Didem Arslantas. 2014. “Assessment of Internet Addiction and Loneliness in Secondary and High School Students.” *JPMA. The Journal of the Pakistan Medical Association* 64 (9): 998–1002.

Livingstone, S, and L Haddon. 2009. “EU Kids Online: Final Report.”

Livingstone, Sonia. 2013. “Online Risk, Harm and Vulnerability: Reflections on the Evidence Base for Child Internet Safety Policy.” *ZER: Journal of Communication Studies* 18 (35): 13–28.

Livingstone, Sonia, Julia Davidson, Joanne Bryce, and Saqba Batool. 2017. “Children’s Online Activities, Risks and Safety A Literature Review by the UKCCIS Evidence Group.” UKCCIS Evidence Group.

Livingstone, Sonia, Anke Görzig, and Kjartan Ólafsson. 2011. “Disadvantaged Children and Online Risk.” Monograph. http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx.

Livingstone, Sonia, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2010. “Risks and Safety for Children on the Internet: The UK Report: Full Findings from the EU Kids Online Survey of UK 9-16 Year Olds and Their Parents.” Monograph. http://www.eukidsonline.net/.

———. 2011a. “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.” Monograph. 2011. http://www.eukidsonline.net/.

———. 2011b. “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.” Monograph. 2011. http://www.eukidsonline.net/.

———. 2011c. “Technical Report and User Guide: The 2010 EU Kids Online Survey.” EU Kids Online.

Livingstone, Sonia, Leslie Haddon, Jane Vincent, Giovanna Mascheroni, and Kjartan Ólafsson. 2014. “Net Children Go Mobile The UK Report.” http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/NCGMUKReportfinal.pdf.

Livingstone, Sonia, and Ellen Helsper. 2010a. “Balancing Opportunities and Risks in Teenagers’ Use of the Internet: The Role of Online Skills and Internet Self-Efficacy.” *New Media & Society* 12 (2): 309–29. https://doi.org/10.1177/1461444809342697.

———. 2010b. “Balancing Opportunities and Risks in Teenagers’ Use of the Internet: The Role of Online Skills and Internet Self-Efficacy.” *New Media & Society* 12 (2): 309–29. https://doi.org/10.1177/1461444809342697.

———. 2010c. “Balancing Opportunities and Risks in Teenagers’ Use of the Internet: The Role of Online Skills and Internet Self-Efficacy.” *New Media & Society* 12 (2): 309–29. https://doi.org/10.1177/1461444809342697.

Livingstone, Sonia, Giovanna Mascheroni, Kjartan Ólafsson, and Leslie Haddon. 2014. “Children’s Online Risks and Opportunities: Comparative Findings from EU Kids Online and Net Children Go Mobile.” EU Kids Online and Net Children Go Mobile.

Livingstone, Sonia, 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): 635–54.

Magkos, Emmanouil, Eleni Kleisiari, Panagiotis Chanias, and Viktor Giannakouris-Salalidis. 2014. “Parental Control and Children’s Internet Safety: The Good, the Bad and the Ugly.”

Martin, Florence, Chuang Wang, Teresa Petty, Weichao Wang, and Patti Wilkins. 2018. “Middle School Students’ Social Media Use.” *Educational Technology & Society*, 213–224.

Mascheroni, Giovanna, and Kjartan Ólafsson. 2014. “Net Children Go Mobile: Risks and Opportunities.” Monograph. February 2014. http://www.netchildrengomobile.eu.

Miller, Cody, and Gabby Hart. 2019. “Authorities Warn Parents, Children of Scams Targeting ‘Fortnite’ Gamers.” 3 News LAS VEGAS. 2019. https://news3lv.com/news/local/authorities-warn-parents-children-of-scams-targeting-online-game-fortnite.

Mobicip. n.d. “Mobicip Features.” https://www.mobicip.com/features.

“Net Nanny Parental Control Overview.” n.d. Net Nanny. Accessed January 5, 2017. https://www.netnanny.com/features/.

NSPCC. n.d. “Online Safety.” NSPCC. Accessed November 17, 2016. https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/.

Nurse, Jason. 2013. “Effective Communication of Cyber Security Risks.”

Ofcom. 2014a. “Children’s Online Behaviour: Issues of Risk and Trust Qualitative Research Findings.” Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0028/95068/Childrens-online-behaviour-issues-of-risk-and-trust.pdf.

———. 2014b. “Children’s Online Behaviour: Issues of Risk and Trust Qualitative Research Findings.” Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0028/95068/Childrens-online-behaviour-issues-of-risk-and-trust.pdf.

———. 2016. “Children and Parents: Media Use and Attitudes Report 2016.” Ofcom. https://www.ofcom.org.uk/research-and-data/media-literacy-research/children/children-parents-nov16.

———. 2019a. “Children and Parents Media Use and Attitudes: Annex 1.” https://www.ofcom.org.uk/__data/assets/pdf_file/0027/134892/Children-and-Parents-Media-Use-and-Attitudes-Annex-1.pdf.

———. 2019b. “Children’s Media Use and Attitudes Report 2019 – Research Annex.” https://www.ofcom.org.uk/__data/assets/pdf_file/0024/190518/children-media-use-attitudes-2019-chart-pack.pdf.

———. 2020. “Internet Users’ Experience of Potential Online Harms: Summary of Survey Research.” Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0024/196413/concerns-and-experiences-online-harms-2020-chart-pack.pdf.

Oksanen, Atte, Matti Näsi, Jaana Minkkinen, Teo Keipi, Markus Kaakinen, and Pekka Räsänen. n.d. “Young People Who Access Harm-Advocating Online Content: A Four-Country Survey.” *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 2016.

Ólafsson, Kjartan, Sonia Livingstone, and Leslie Haddon. 2014. “Children’s Use of Online Technologies in Europe: A Review of the European Evidence Base.” http://eprints.lse.ac.uk/60221/.

Papadaki, M, and SM Furnell. 2006. “Achieving Automated Intrusion Response: A Prototype Implementation.” *Information Management & Computer Security*, 235–51.

“Parental Control Software - Norton Family.” n.d. Norton. Accessed January 7, 2017. https://family.norton.com/web/.

Pons-Salvador, Gemma, Xud Zubieta-Méndez, and Dolores Frias-Navarro. 2018. “Internet Use by Children Aged Six to Nine: Parents’ Beliefs and Knowledge about Risk Prevention.”

Priestlands School. 2016. “Posting Videos on YouTube and Other Online Platforms.” Priestlands School. 2016. http://www.priestlands.hants.sch.uk/Posting-videos-on-YouTube-and-other-online-platforms.

Pustovalova, Alexandra. 2016. “How to Manage Your Kid’s Screen Time with Kaspersky Safe Kids.” 2016. https://www.kaspersky.com.au/blog/safe-kids-time-limits/11214/.

Qustodio. n.d. “Qustodio Premium.” https://www.qustodio.com/en/premium-special-promo-b/?utm_source=google&utm_medium=cpc&utm_term=brand&utm_campaign=adw_ww_web_brand___brand_ww&gclid=CjwKCAiA35rxBRAWEiwADqB372IphUgOv5KNAYctQkzwD-ZQWZtqu4ODDdBZb6BvD4tq5WmSpknX3xoCa5AQAvD_BwE.

Rideout, Vicky. 2016. “Measuring Time Spent with Media: The Common Sense Census of Media Use by US 8- to 18-Year-Olds.” *Journal of Children and Media* 10 (1): 138–44. https://doi.org/10.1080/17482798.2016.1129808.

Rubenking, Neil J. 2018. “Norton Family Premier.” 2018. https://us.norton.com/norton-family-premier.

Rubenking, Neil J., and Ben Moore. 2019. “The Best Parental Control Software for 2020.” 2019. https://www.pcmag.com/picks/the-best-parental-control-software.

Sandhu, Ravneet. 2015. “Cyberbullying in Video Games.” Beyond Bullies. 2015. http://beyondbullies.org/2015/02/cyberbullying-video-games/.

Santisarun, Phakpoom, and Sirapat Boonkrong. 2015. “Social Network Monitoring Application for Parents with Children under Thirteen.” *In Knowledge and Smart Technology (KST), 2015 7th International Conference On*, 75–80.

Scott, Jennifer. 2016. “Children and the Internet: An Exploration of Year 5 Pupils’ Online Experiences and Perceptions of Risk.” *Fields: Journal of Huddersfield Student Research* 2 (1): e21. https://doi.org/10.5920/fields.2016.2121.

Sharma, Akhilesh. n.d. “How Hackers Hack Facebook Account & How to Stop Them?” Tweak And Trick. Accessed November 21, 2016. http://www.tweakandtrick.com/2011/05/hack-facebook-account-password.html.

Shu Ching Yang. 2012. “Paths to Bullying in Online Gaming: The Effects of Gender, Preference for Playing Violent Games, Hostility, and Aggressive Behavior on Bullying.” *Journal of Educational Computing Research* 47 (3): 235–49. https://doi.org/10.2190/EC.47.3.a.

“Signs and Symptoms of Internet or Computer Addiction.” n.d. PsychGuides. Accessed November 21, 2016. http://www.psychguides.com/guides/computerinternet-addiction-symptoms-causes-and-effects/.

Sithira, V., and Yok-Yen Nguwi. 2014. “A Study on the Adolescent Online Security Issues.” *International Journal of Multidisciplinary and Current Research* 2: 596–601.

Smahel, D., H. Machackova, G. Mascheroni, L. Dedkova, E. Staksrud, K. Ólafsson, S. Livingstone, and U. Hasebrink. 2020. “EU Kids Online 2020: Survey Results from 19 Countries.” EU Kids Online. https://doi.org/10.21953/lse.47fdeqj01ofo.

Staksrud, Elisabeth, Kjartan Ólafsson, and Sonia Livingstone. 2013a. “Does the Use of Social Networking Sites Increase Children’s Risk of Harm?” *Computers in Human Behavior* 29 (1): 40–50.

———. 2013b. “Does the Use of Social Networking Sites Increase Children’s Risk of Harm?” *Computers in Human Behavior* 29 (1): 40–50.

Stald, Gitte Bang, Leila Green, Monica Barbowski, Leslie Haddon, Giovanna Mascheroni, Bence Sagvari, Barbara Scifo, and Liza Tzaliki. 2014. “Online on the Mobile: Internet Use on the Smartphone and Associated Risks among Youth in Europe.” http://forskningsbasen.deff.dk/Share.external?sp=Sbdb50d45-43d0-4527-bacf-e6d3c8028c1f&sp=Situ.

Stephenson, Michael T., Rick H. Hoyle, Philip Palmgreen, and Michael D. Slater. 2003. “Brief Measures of Sensation Seeking for Screening and Large-Scale Surveys.” *Drug and Alcohol Dependence* 72 (3): 279–86. https://doi.org/10.1016/j.drugalcdep.2003.08.003.

Steyer, James. 2014. “Parents, Take Heed: ‘Slenderman’ and More Lurk Online.” CNN. 2014. https://edition.cnn.com/2014/06/04/opinion/steyer-slenderman-kids-media/index.html.

Stroud, Carl. 2017. “PUPPET ‘DANGER’ YouTube Puppet Sensation Jeffy ‘Taught My Kid How to Put a Noose around His Neck.’” The Sun. 2017. https://www.thesun.co.uk/news/5119897/youtube-puppet-jeffy-taught-child-put-noose-around-neck/.

Symons, Katrien, Koen Ponnet, Kathleen Emmery, Michel Walrave, and Wannes Heirman. 2016. “Parental Knowledge of Adolescents’ Online Content and Contact Risks.” *Journal of Youth and Adolescence*, November, 1–16. https://doi.org/10.1007/s10964-016-0599-7.

“The Internet’s Best Free Parental Control App.” n.d. Qustodio. Accessed January 6, 2017. https://www.qustodio.com/en/.

Theoharidou, Marianthi, Alexios Mylonas, and Dimitris Gritzalis. 2012. “A Risk Assessment Method for Smartphones.” In *IFIP International Information Security Conference*, 443–456. Springer. http://link.springer.com/10.1007/978-3-642-30436-1_36.

Third, Amanda, Delphine Bellerose, Urszula Dawkins, Emma Keltie, and Kari Pihl. 2014. “Children’s Rights in the Digital Age.” http://www.unicef.org/publications/files/Childrens_Rights_in_the_Digital_Age_A_Download_from_Children_Around_the_World_FINAL.pdf.

Tsitsika, Artemis, Mari Janikian, Tim M. Schoenmakers, Eleni C. Tzavela, Kjartan Olafsson, Szymon Wójcik, George Florian Macarie, Chara Tzavara, and Clive Richardson. 2014. “Internet Addictive Behavior in Adolescence: A Cross-Sectional Study in Seven European Countries.” *Cyberpsychology, Behavior and Social Networking* 17 (8): 528–35. https://doi.org/10.1089/cyber.2013.0382.

UNICEF Innocenti Research Centre. 2011. “Child Safety Online Global Challenges and Strategies.”

Valcke, M., B. De Wever, H. Van Keer, and T. Schellens. 2011. “Long-Term Study of Safe Internet Use of Young Children.” *Computers & Education* 57 (1): 1292–1305. https://doi.org/10.1016/j.compedu.2011.01.010.

Vandoninck, Sofie, Leen D’Haenens, and Keith Roe. 2013. “Online Risks: Coping Strategies of Less Resilient Children and Teenagers across Europe.” In . https://doi.org/10.1080/17482798.2012.739780.

Wagenseil, Paul. 2020. “Best Parental Control Apps for Android and IPhone 2020.” 2020. https://www.tomsguide.com/us/best-parental-control-apps,review-2258.html.

Wallace, Kelly. 2014. “Slenderman Stabbing Case: When Can Kids Understand Reality vs. Fantasy?” CNN. 2014. https://edition.cnn.com/2014/06/03/living/slenderman-stabbing-questions-for-parents/index.html.

Wang, Yang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Faith Cranor. 2013. “Privacy Nudges for Social Media: An Exploratory Facebook Study.” In , 763–70. ACM Press. https://doi.org/10.1145/2487788.2488038.

Publications

Alotaibi, M., Furnell, S., Papadaki, M., and Atkinson, S. (2018). "Using Risk Communication for Improving Parental Control Features". International Conference on Information Society (i-Society 2018), Dublin, Ireland, pp. 40-47. (ISBN: 978-1-908320-92-6). DOI: 10.2053/iSociety.2018.0006

Abstract

The Internet is growing rapidly and is becoming an essential part of children's lives. Internet use has many benefits for learning, participation, creativity, entertainment and communication. Along with the benefits, however, the Internet use might expose children to a wide range of online risks, some of them are known in the offline world such as bullying, pornography, sexual exploitation, and the viewing of inappropriate content, such as scenes of violence and suffering. There are also new risks such as invasion of personal data and privacy, geo-location tracking, sexual messaging and harassment. This paper presents a review of children's Internet use and the online risks and threats. Also, the efforts that have been introduced to guarantee online safety for young people are presented. Unfortunately, the existing mechanisms for protecting children online are not effective. Parents do not always understand the potential risks their children may encounter. Furthermore, the current parental controls focus on monitoring and restrictive functions to reduce online risks, which might not satisfy the expectations of young people who want unrestricted freedom to use Internet. In addition, children need to be aware of Internet safety and how to cope with the risk and harm they may encounter. As a result, the paper proceeds to consider risk communication technologies as a first step to raise awareness about the potential risks for parents and children. This paper aims to integrate risk communication strategy with the parental controls. The proposed risk communication framework for improving awareness about the potential online risk for parents and children is presented. Risk communication technologies might be the best way to raise risk awareness for parents and children, and help them to make a safe decision.

Alotaibi, M., Furnell, S., Papadaki, M., and Atkinson, S. (2019). "A risk assessment model for children's Internet use", in Proceedings of 18th Annual Security Conference (ASC2019, Las Vegas, NV, April 2019.

Abstract

The increased use of the Internet by young people have created many new opportunities for learning, participation, creativity, entertainment and communication. On the other hand, it also present various threats and risks such as bullying, pornography, or sexual exploitation. Young people might be more vulnerable to risks, although not all risk leads to harm. They could engage in some online behaviours that expose them to risk. Unfortunately, parents do not always understand the potential risks their children may encounter. Furthermore, young people are unaware of the online risks and the implications associated with their online activities. Thus, there is a need for risk assessment solutions that focus on assessing different risk levels of child's internet use. Therefore, this paper presents a risk assessment model that assesses risk levels of children online activities to warn parents and children in an individualized, timely and continuous way. Risk value is calculated as a combination of likelihood and impact. The risk likelihood is computed using the factors that forms children online experiences: child's activity type, and child's Internet access and use. The impact consequences for each activity could be assessed by parents. Thus, this model helps parents to understand and assess online risks and aims to support them in safeguarding their children.

Appendices

Appendix A: Ethical approval letter, research information sheet, consent form, and invitation

Ethical approval letter

UNIVERSITY OF PLYMOUTH

22 January 2019

CONFIDENTIAL
Moneerah Alotaibi
School of Computing, Electronics and Mathematics

Dear Moneerah

Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

Using risk communication for improving parental control features

I am pleased to inform you that this has been approved.

Kind regards

Steven Neal
Secretary to Faculty Research Ethics Committee

Cc. Prof Steven Furnell

Mrs Jayne Brenen, Head of Faculty Operations, Faculty of Science and Engineering, University of Plymouth, Drake Circus, Plymouth, Devon PL4 8AA T +44 (0)1752 584584 F +44 (0)1752 584540 W www.plymouth.ac.uk

Information sheet

SAMPLE INFORMATION SHEET FOR ADULT / CHILD

PLYMOUTH UNIVERSITY

FACULTY OF SCIENCE AND ENGINEERING

RESEARCH INFORMATION SHEET

Name of Principal Investigator

Moneerah Alotaibi

Title of Research

Using Risk Communication for Improving Parental Control Features

Aim of research

The aim of the research is to develop a system for raising security awareness for parents and children through using risk communication mechanism. The system uses a risk assessment model to recognise, and calculate risk levels for each child's activity, to inform parents and children when there is a probability of exposure to online risk and to find ways to avoid those risks.

Description of procedure

The developed system requires an evaluation from the stakeholder community (i.e. parents) with the purpose to collect users' opinions about system design and the functionality, and to identify its strengths, weaknesses and limitations. This will involve watching a show of the prototype tool, then doing some tasks using the proposed system, and filling in a questionnaire to gather their feedback.

All interview sessions will be conducted in computer lab within the Centre for Security, Communications and Network Research (CSCAN). Total amount of time needed for each session will vary between 30 and 50 minutes depending on the tasks, questions and discussion. All sessions will be recorded (audio-video recording) with the parent's prior permission for later analysis. Records will be deleted once the feedback is transcribed.

Description of risks

All of the information will be treated confidentially and data will be anonymous during the collection, storage and publication of research material.

Benefits of proposed research

The objective of this research is to integrate parental controls with security awareness initiatives to raise awareness for parents and children and help them to make safe decisions. Parents need to be aware of their children's online activities and risk levels associated with those activities. Thus, the proposed system aims to monitor children's online activities to inform parents and children when there is a probability of exposure to online risk and to find ways to avoid those risks.

Right to withdraw

You have the right to withdraw at any time during the interview session.

If you are dissatisfied with the way the research is conducted, please contact the principal investigator in the first instance: telephone number [07463991992]. If you feel the problem has not been resolved please contact the secretary to the Faculty of Science and Engineering Human Ethics Committee: Mrs Paula Simson 01752 584503.

Consent form

SAMPLE SELF-CONSENT FORM

PLYMOUTH UNIVERSITY

FACULTY OF SCIENCE AND ENGINEERING

Human Ethics Committee Sample Consent Form

CONSENT TO PARICIPATE IN RESEARCH PROJECT / PRACTICAL STUDY

Name of Principal Investigator

Moneerah Alotaibi

Title of Research

Using Risk Communication for Improving Parental Control Features

Brief statement of purpose of work

The internet is growing rapidly and becoming an essential part of children's lives. The use of the Internet is deemed important for learning, communication, and entertainment. Despite the benefits, the use of the Internet exposes young people to an array of online risks, such as bullying, sexual exploitation.

Thus, the aim of the research is to develop a system for raising security awareness for parents and children through using risk communication mechanism. The system uses a risk assessment model to recognise and calculate risk levels for each child's activity, to inform parents and children when there is a probability of exposure to online risk and to provide ways to avoid those risks.

The developed system requires an evaluation from the stakeholder community (i.e. parents) with the purpose to collect users' opinions about system design and the functionality, and to identify its strengths, weaknesses and limitations. As such, I would be grateful for your participation. This will inwolve watching a show of the prototype tool, then doing some tasks using the proposed system, and filling in a questionnaire to gather your feedback.

You have the right to withdraw at any stage of this evaluation process. Should you wish to do so, please contact Moneerah Alotaibi.

For information regarding the study, please contact:
Moneerah Alotaibi – moneerah.alotaibi@plymouth.ac.uk

For any questions concerning the ethical status of this study, please contact the secretary of the Human Ethics Committee – paula.simson@plymouth.ac.uk

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far as possible, to avoid any risks, and that safety and health risks will have been separately assessed by appropriate authorities (e.g. under COSHH regulations) Under these circumstances, I agree to participate in the research.

Name: .....

Signature: ..... Date: .....

Invitation

Parents needed to participate in a Research Study

We are looking for parents (of children aged between 4 and 16) to take part in a study relating to children's use of mobile devices and their awareness of associated risks.

The aim of the research is to develop a system for raising security awareness for parents and children through using a risk communication mechanism. The system calculates risk levels for a child's activity, and then can inform parents and children of probable risk exposure and ways to avoid them.

We are looking for parents to help with the evaluation of a prototype of the system, so that we can collect parents' opinions about system design and the functionality, and to identify its strengths, weaknesses and limitations. This will involve watching a demonstration of the tool, and then doing some tasks with it, and filling in a questionnaire to gather their feedback.

The total amount of time needed for the session will be between 30 - 50 minutes depending on the tasks, questions and discussion. The session will be recorded (subject to parent's prior permission) for later analysis. These recordings will be deleted once the feedback is transcribed.

All of the information will be treated confidentially, and data will be anonymous during the collection, storage and publication of research material. Participants will have the right to withdraw at any time during the session.

A £15 payment will be offered upon completion of the study.

If you are willing to participate, please contact me to arrange a slot:
Moneerah Alotaibi (PhD researcher) moneerah.alotaibi@plymouth.ac.uk or 00447463991992

Thank you!

This study has been reviewed and approved by the University of Plymouth's Ethical Principles for Research Involving Human Participants.

Appendix B: Task scenarios

Initial task scenario

The Internet is becoming an essential part of children's lives. Internet use provides a wealth of opportunities for learning, participation, creativity, entertainment and communication. On the other hand, it also present various risks, although not all risk leads to harm. Children's online activities could expose them to different risk levels: low, medium, or high.

The parental control application aims to monitor child's online activities and assess the risks associated with children's Internet use in order to warn parents and children to avoid these risks.

Task 1:

Different online activities could cause different risk levels (low, medium, or high). The system allows you to assign general protection responses that will be taken when low-, medium-, or high-risk events occur. The protection responses include controlling the activity (allow, or block), alerting parents, or sending advice to the child.

In this scenario, you are the parent of 12-year-old Emily, who uses the Internet. Emily conducts different online activities that could involve various risk levels (low, medium, or high). Thus, the system helps you to assign general protection responses that will be taken when low-, medium-, or high-risk events occur. In this situation, you are concerned about high-risk events and you want to check the responses that will be taken when these occur.

Please use the system to access Emily's account and general response settings for different risk levels and determine the appropriate protection response(s) required for a high-risk event.

What protection response(s) would you assign in the system for high-risk events?

Protection response: 1. Control the activity

2. Alert

3. Issue awareness-raising for the child

4. Limit application use

Task 2:

Children's online activities have various risk levels. Therefore, the system enables you to assess the risk level of an activity and its impacts and customize appropriate protection responses.

In this scenario, you are concerned about Emily's activities, such as her ability to access inappropriate content. Please use the system to access Emily's account and activity controls and determine the risk level for general access to inappropriate content across all applications and the protection responses.

What risk level would you assign in the system for access to inappropriate content activity?

Risk level of access to inappropriate content

What protection response(s) would you assign in the system for access to inappropriate content activity?

Protection response: 1. Control the activity

2. Alert

3. Issue awareness-raising for the child

4. Limit application use

Refined task scenario

Task 1:

In this scenario, you are the parent of 12-year-old Emily, who uses the Internet and could be at different risk levels (low, medium, or high).

You are concerned about Emily and you want to know the protection responses for high-risk events.

Please use the system to access Emily's account:

- Check the general risk response(s) assigned for a high-risk event (such as allowing of the child's activity, receiving an alert, issuing awareness-raising for the child, and limiting application use), if you are not happy with default protection response(s), you can change them.

Task 2:

In this scenario, you are concerned about Emily's activities such as accessing to inappropriate content. Thus, you want to assess the risk level of accessing to inappropriate content, and want to know the protection responses for this activity.

Please use the system to access Emily's account and activity –specific settings.

1- Check the current risk level setting of general access to inappropriate content (low, medium, or high) and impacts (such as child's safety, child's social relationships, child's privacy, financial loss, and disruption of services), if you are not happy with default settings, you can change them .

2- Check the assigned protection responses for this activity (such as allowing of the child's activity, receiving an alert, issuing awareness-raising for the child, filtering content, and limiting application use), if you are not happy with default settings, you can change them.

Appendix C: Pre-survey questionnaire

A pre-test survey is to be completed at the beginning of the experiment to collect parents' demographic data, children's demographic data, and information about children's Internet use and the parental mediation used. There are four main sections in this survey.

Pre-survey questionnaire before amendments

Section A: Parent's information

1. Age

◯ Under 29 years

◯ 29 - 39 years

◯ 40 - 49 years

◯ 50 - 59 years

◯ 60 years and over

2. Gender

◯ Male

◯ Female

3. Country of origin

4. Education level

◯ None

◯ Primary school

◯ Secondary school

◯ College or university

5. How often do you use the Internet?

◯ Several times a day

◯ Several times a week

◯ Once a week

◯ Once a month or less

Section B: Child's information

6. Child's age

◯ 4 - 7 years

◯ 8 - 11 years

◯ 12 - 16 years

7. Child's gender

◯ Boy

◯ Girl

8. Is your child sensation-seeking (e.g., doing dangerous things for fun)?

◯ Yes

◯ No

9. Does your child have psychological difficulties?

◯ Yes

◯ No

Section C: Child's Internet use

10. How old was your child when he/she first used the Internet?

11. How often does your child use the Internet?

◯ Several times a day

◯ Several times a week

◯ Once a week

◯ Do not know

12. Which of these devices does your child usually use for the Internet access?

☐ Shared handheld device (e.g., smartphone, iPod, iPad)

☐ Own handheld device (e.g., smartphone, iPod, iPad)

☐ Shared laptop

☐ Own laptop

☐ Shared desktop computer

☐ Own desktop computer

☐ Other (please specify)

13. Where does your child usually use the Internet?

☐ Private rooms, e.g., bedroom

☐ Public room in the home

☐ School

☐ Other (please specify)

14. To what extent are you concerned about your child's online behaviour?

◯ Not concerned

◯ Somewhat concerned

◯ Very concerned

If not, why not?

15. If yes, which of the following has your child done? And to what extent are you concerned about these online activities and their consequences?

Online activities	Child has done	Level of parental concern about the child's activities	Potential consequences of the activity (i.e., in terms of child's safety, privacy, or financial loss)
Using a web browser	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Using file-sharing platforms	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Playing multiplayer games	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact

Using communication platforms (e.g., social networks, chatrooms, or email)	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Accessing inappropriate content	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Accepting people as friends without knowing them offline	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Inappropriate chatting	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Sharing personal information with unknown people	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Using a camera/ microphone with unknown people	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Making app purchases	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Downloading inappropriate applications	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Spending too much time on the Internet	◯ Yes ◯ No ◯ Do not know	◯ Not concerned ◯ Somewhat concerned ◯ Very concerned	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact

Section D: Parental controls

28. If you are concerned about your child's online activities, do you use parental mediation to manage your concern?

◯ Yes

◯ No

If not, why not?

29. If yes, which type(s) of parental mediation have you used?

☐ Active mediation (the parent is staying nearby, discussing the child's online activities, and guiding for using the Internet safely).

☐ Restrictive mediation (parent sets rules that restrict the child's use, such as the child is not permitted to share personal information on the Internet).

☐ Monitoring (the parent checks available records of the child's Internet use afterwards).

☐ Technical mediation (the parent uses parental control software to restrict or monitor the child's use).

Other comments

Please if you use technical mediation (parental control application), answer the following questions

30. Which parental control application do you use?

31. How long have you been using it?

◯ Up to one year

◯ One to three years

◯ More than three years

Other comments

32. What do you use the parental control app for?

☐ Monitoring the child's online activities.

☐ Restricting the child's online activities (content restriction, chat restriction, or time restriction)

Other comments

33. How satisfied are you with the functions provided by this app (e.g., do you find the functions provided by the app helpful)?

◯ Very Satisfied

◯ Satisfied

◯ Neutral

◯ Dissatisfied

◯ Very Dissatisfied

Other comments

Pre-survey questionnaire after amendments (the changes in Question 15)

15. Which of the following has your child done? What is the risk level of each activity? And to what extent are you concerned about these online activities?

Online activities	Child has done	Activity risk level	Parental concern about the activity
Using a web browser	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned
Using file-sharing platforms	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned
Playing multiplayer games	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned
Using communication platforms (e.g., social networks, chatrooms, or email)	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned
Accessing inappropriate content	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned

Accepting people as friends without knowing them offline	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned
Inappropriate chatting	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned
Sharing personal information with unknown people	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned
Using a camera/ microphone with unknown people	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned
Making app purchases	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned
Downloading inappropriate applications	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned
Spending too much time on the Internet	◯ Yes ◯ No ◯ Do not know	◯ No risk ◯ Low risk activity ◯ Moderate risk activity ◯ High risk activity	◯ Not concerned ◯ Concerned

16. To what extent could the following online activities affect the child on the following aspects:

Online activities	Impact consequences				
	Child's safety	Child's social relationships	Child's privacy	Financial loss	Disruption of services of applications
Using web browsers	◯ No impact ◯ Low impact	◯ No impact ◯ Low impact	◯ No impact ◯ Low impact	◯ No impact ◯ Low impact ◯ Medium impact	◯ No impact ◯ Low impact

	◯ Medium impact ◯ High impact	◯ Medium impact ◯ High impact	◯ Medium impact ◯ High impact	◯ High impact	◯ Medium impact ◯ High impact
Using file-sharing platforms	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Playing multiplayer games	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Using com-munication platforms (e.g., social networks, chatrooms, or email)	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Accessing inap-propriate content	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Accepting people as friends without knowing them offline	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Inap-propriate chatting	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Sharing personal information with unknown people	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Using a camera/ microphone with unknown people	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact

Making purchases	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Down-loading inap-propriate applications	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact
Spending too much time on the Internet	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact	◯ No impact ◯ Low impact ◯ Medium impact ◯ High impact

Appendix D: Post-survey questionnaire

Post survey was completed at the end of the experiment, which aims to get participants' feedback on their perceptions about the system's usefulness and usability.

Post-survey questionnaire

Thank you for using the tool. Please take a minute or two to give us your opinion and feedback in order to enhance the proposed tool.

1. Do you understand the concept of the proposed system (i.e., calculating and predicting the risk levels of children's online activities in order to warn parents and protect children online)?

◯ Very clear

◯ Clear

◯ Moderately clear

◯ Confusing

◯ Very confusing

2. What is your opinion of the system? Please rate how much you agree or disagree with the following statements:

	Strongly agree	Agree	Not sure	Disagree	Strongly disagree
The overall appearance of the system is suitable	◯	◯	◯	◯	◯
The amount of information seems appropriate and sufficient	◯	◯	◯	◯	◯
The concepts / terms in the system are clear	◯	◯	◯	◯	◯
It's clear how to assign general protection responses for different risk events (low, medium, and high)	◯	◯	◯	◯	◯
It's clear how to assess the risk level of an activity and customize specific appropriate protection responses	◯	◯	◯	◯	◯
Overall, the system is easy to use	◯	◯	◯	◯	◯
The issued alert is understandable and informative	◯	◯	◯	◯	◯
The functions provided by system are appropriate and adequate	◯	◯	◯	◯	◯

Other comments

3. Would you use this system in real life?

◯ Yes

◯ No

If not, why not?

4. Do you have any further comments (e.g., what do you like or not like about the system)?

5. What other functions could be added to the app to improve its effectiveness?

Appendix E: Participants' assessment of the risk level of their children's online activities in different age groups

Activities risk level assessment by child's age

Activities	**4-7**					**8-11**					**12-16**				
	Activity risk level according to parents' view				**Activity risk level (mode)**	**Activity risk level according to parents' view**				**Activity risk level (mode)**	**Activity risk level according to parents' view**				**Activity risk level (mode)**
	No risk	**L**	**M**	**H**		**N**	**L**	**M**	**H**		**N**	**L**	**M**	**H**	
Using web browsers	3	3	3	3	-	0	2	1	1	L	4	11	9	6	L
Using communication platforms (e.g., social networks, chatrooms, or email)	2	1	5	4	M	1	0	1	2	H	0	2	3	9	H
Playing multiplayer games	2	4	6	0	M	0	1	3	0	M	2	2	4	6	H
Using file-sharing platforms	3	2	4	3	M	0	2	2	0	L M	3	1	7	3	M
Making an app purchase	2	5	5	0	L-M	0	1	3	0	M	2	4	4	4	-
Accessing inappropriate content	3	1	3	5	H	0	0	1	3	H	3	1	2	8	H
Accepting people as friends without knowing them offline	3	1	1	7	H	0	0	4	0	M	3	1	3	7	H
Inappropriate chatting with people	4	0	0	8	H	0	0	1	3	H	2	1	4	7	H
Sharing personal information with unknown people	3	0	2	7	H	0	0	2	2	M H	3	1	3	7	H
Using a camera/microphone with unknown people	3	1	0	8	H	0	0	0	4	H	3	3	1	7	H
Downloading inappropriate applications	2	1	4	5	H	0	0	2	2	M H	4	1	4	5	H
Spending too much time on the Internet	0	4	6	2	M	0	1	2	1	M	0	2	6	6	M H