Guidelines for Parents, Guardians and Educators on Child Online Protection

Second Edition, 2016

www.itu.int/cop

ACKNOWLEDGEMENTS

These Guidelines have been prepared by ITU and a team of contributing authors from leading institutions active in the ICT sector and would not have been possible without their time, enthusiasm and dedication.

ITU is grateful to all of the following authors, who have contributed their valuable time and insights: (listed in alphabetical order of organisation)

- John Carr (Children's Charities' Coalition on Internet Safety)
- Margareta Traung (European Commission Safer Internet programme)
- Isabella Santa (European Network and Information Security Agency)
- Janice Richardson (Insafe network)
- Cristina Bueti and Sandra Pandi (ITU)
- Nevine Tewfik (The Suzanne Mubarak Women's International Peace Movement: CyberPeace Initiative)
- Ethel Quayle (University of Edinburgh, United Kingdom)

The authors wish to thank John Carr from CHIS, Sonia Billard and Christiane Agbton-Johnson from UNIDIR, and Katerina Christaki from ENISA for their detailed review and comments.

ITU wishes to acknowledge Salma Abbasi from eWWG for her valuable involvement in the Child Online Protection (COP) Initiative.

The second edition has been updated by Neha Karkara.

Additional information and materials relating to these Draft Guidelines can be found at: http://www.itu.int/cop/ and will be updated on a regular basis. If you have any comments, or if you would like to provide any additional information, please contact Ms JeoungHee Kim at cop@itu.int.

Table of Contents


“
Protecting children online is a global issue, so a global response is needed
”

Foreword

It is my pleasure to share with you the 2016 update of the Child Online Protection Guidelines.This version was updated at the request of the Member States within the framework of the Regional Initiative on COP, approved by the World Telecommunication Development Conference (WTDC-2014). I would like to thank the various partners who contributed to their development. In an era of 'always on-line' it is a critical issue which, with the borderless nature of the Internet, requires a global, coordinated response. Parents, educators, industry and policy makers are key in ensuring children's safety online, and I am personally grateful for your support

Houlin Zhao

Secretary-General of
the International Telecommunication Union (ITU)

Executive Summary

The Internet has brought untold benefits to children around the world, with the number of connected households increasing each year. In 2015, there are globally 3.2 billion people using the Internet, as oppose to 1.5 billion in early 2009[1]. But while the potential for good is undisputed, the Internet has also raised some new and disturbing issues, especially where children are concerned.

Today's youth are very technically savvy. They are able to master complex programmes and applications quickly and easily on both computers and mobile or other personal devices and they seem to be able to do this almost intuitively. On the other hand, when it comes to computer programmes and mobile or personal devices, adults in general tend to require an instruction manual for what most children would say are fairly simple tasks. However, what adults can bring to the e-safety debate are invaluable life skills and experience.

It is crucial to establish what children and young people are actually doing online as opposed to what adults think they are doing. Research is showing that more and more children are connecting to the Internet using mobile phones, tablets and other handheld devices such as iPod Touch, e-book readers and games consoles. A study in UK shows the use of tablets has tripled in 2014, becoming the device of choice for 8 to 11 year olds to access audio-visual content and games in particular. Over six in ten 12-15 years olds now own a smartphone and it is the most popular device for social

1 http://www.itu.int/net/pressoffice/press_releases/2015/17.aspx#.VkVnTYTNyf4 (Accessed 12 November 2015)

networking among that age group.[2]

One key issue is that many parents and guardians adhere to the common misconception that their children are safer if they are at home using a computer, or at school, than they would be if they were accessing the Internet outside of the home. This is a dangerous misconception because the Internet can take children and young people virtually anywhere in the world, and in the process they can be exposed to potentially dangerous risks, just as they could in the real world. Moreover children and young people experience slightly increased risk of harm when accessing the Internet via a smartphone, tablet or another handheld device. This is because these handheld devices give instant access to the Internet from anywhere and are less likely to be monitored by parents or caregivers.

These Guidelines have been developed within the Child Online Protection (COP) Initiative[3], as part of ITU's Global Cybersecurity Agenda[4], with the aim of establishing the foundations for a safe and secure cyberworld not only for today's youth but also for future generations.

The Guidelines are meant to act as a blueprint which can be adapted and used in a way which is consistent with national or local customs and laws. Moreover, it will be appreciated that these guidelines address issues which might affect all children and young people under the age of 18 but each age group will have different needs.

Indeed each child is unique, deserving individual consideration.

These Guidelines have been prepared by ITU in a very collaborative way involving a team of contributing authors from leading institutions active in the ICT sector, namely EU Safer Internet Programme, European Network and Information Security Agency (ENISA)[5], Children's Charities' Coalition on Internet Safety, Cyberpeace Initiative and the University of Edinburgh (United Kingdom). Invaluable contributions were also received from individual national governments and high technology companies who share a common objective of making the Internet a better and safer place for children and young people.

ITU, together with the other authors of this report is calling

2 Ofcom Report on Internet safety measures, Strategies of parental protection for children online, 2014, Available at http://stakeholders.ofcom.org.uk/binaries/internet/internet-safety-measures.pdf (accessed 13 November 2015)

3 http://www.itu.int/cop

4 http://www.itu.int/osg/csd/cybersecurity/gca/

5 http://www.enisa.europa.eu

upon all stakeholders to promote the adoption of policies and strategies that will protect children in cyberspace and promote safe access to online resources. This will not only lead to the building of a more inclusive information society, but it will also enable ITU Member States to meet their obligations towards protecting and realizing the rights of children as laid out in the United Nations Convention on the Rights of the Child (CRC)[6], adopted by UN General Assembly (UNGA) resolution 44/25 of 20 November 1989 and the WSIS Outcome Documents (2003-2005)[7], WSIS+10 High Level Event Outcome Documents (2014)[8] and the outcomes of the UNGA Overall Review of the Implementation of the WSIS Outcomes (2015)[9]

The UN Convention on the Rights of the Child defines a child as being any person under the age of 18. These Guidelines address issues facing all persons under the age of 18 in all parts of the world. However, a young internet user of seven years of age is very unlikely to have the same needs or interests as a 12 year old just starting at High School or a 17 year old on the brink of adulthood. At different points in the Guidelines we have tailored the advice or recommendations to these different contexts. Whilst using broad categories can act as a useful guide it should never be forgotten that, in the end, each child is different. Each child's specific needs should be given individual consideration. Moreover there are many different local, legal and cultural factors which could have an important bearing on how these Guidelines might be used or interpreted in any given country or region.

There is now a substantial body of international law and international instruments, which underpin and, in many cases, mandate action to protect children both generally, and also specially in relation to the Internet. Those laws and instruments form the basis of these Guidelines. They are comprehensively summarized in the Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents adopted at the 3rd World Congress against the Sexual Exploitation of Children and Adolescents, in November 2008. Further, the Sustainable Development Goals mandate the Member States to take actions to end all forms of abuse and exploitation of children by 2030, including in cyberspace.

6 http://www.unicef.org/crc

7 http://www.itu.int/wsis/outcome/booklet.pdf

8 http://www.itu.int/net/wsis/implementation/2014/forum/inc/doc/outcome/362828V2E.pdf

9 http://unpan3.un.org/wsis10/

Parents guardians and Educators		
	#	**Key areas for consideration**
1. **A. Safety & security of your personal computer and mobile phones**	a.	1. Keep the computer in a common room
	b.	2. Install firewall and antivirus software
	c.	Install parental control apps in mobiles, use parental control software provided by mobile phone service providers
2. **Rules**	a.	Agree house rules about using the Internet and personal devices, giving particular attention to issues of privacy, age inappropriate places, bullying and stranger danger
	b.	Agree rules about use of mobile and handheld devices.

3. Parents', Guardians' and Teachers' education	a.	Parents, guardians and teachers should be familiar with the Internet sites used by their children and should have a good understanding of how children spend their time online
	b.	Parents, guardians and educators should understand how children use other personal devices such as mobile phones, games consoles, MP3 players, PDAs, etc.
4. Children's education	a.	Educate your children on the risks associated with sharing personal information; arranging face-to-face meetings with a person/`s met online; posting photographs online; making use of the webcam; etc.
5. Communication	a.	Communicate with your children about their experiences


“Adults bring life-skills and experience to the e-safety debate ”

1. Background

The World Summit on the Information Society (WSIS) process and its outcome documents are cornerstones on global policies and frameworks on Internet policy and governance. The two-stage WSIS took place in Geneva (10-12 December 2003) and Tunis (16-18 November 2005), and concluded with a bold commitment "to build a people-centred, inclusive and development-oriented information society, where everyone can create, access, utilize and share information and knowledge" (Geneva Declaration of Principles, Para 1).

At WSIS, ITU was entrusted by leaders of the international community with Action Line C5: "building confidence and security in the use of ICTs". The WSIS Outcomes also specifically recognized the needs of children and young people and their protection in cyberspace. The Tunis Commitment further recognized "the role of information and communication technologies (ICTs) in the protection of children and in enhancing the development of

“Adults bring life-skills and experience to the e-safety debate”

children" as well as the need to "strengthen action to protect children from abuse and defend their rights in the context of ICTs".

The year 2015 marks the 10th anniversary of WSIS. On this occasion the UN General Assembly is all set to evaluate the progress made by WSIS and define its next steps. To this end, the WSIS+10 High-Level Event (that took place in Geneva in 2014) was organized as an extended version of the WSIS Forum. The High Level Event addressed the progress made in the implementation of the WSIS outcomes (2003 and 2005) especially related to the Action Lines, with a view to developing proposals on a new vision beyond 2015 as well as exploring new targets.

The WSIS+10 High Level Event Outcome Documents[1] revised the text of the Action Line C5 while recognizing the importance of the Child Online Protection (COP) Initiative and youth empowerment. It states, "Ensure special emphasis for protection and empowerment of children online. In this regard, governments and other stakeholders should work together to help all enjoy the benefits of ICTs in a safe and secure environment." The document further highlights priority areas to be addressed in the implementation of WSIS beyond 2015. With regard to children's online security it emphasises, "promoting a culture of online security and safety, empowering users, and encouraging national, regional and international cybersecurity strategies to protect users, including children".

Further, the Sustainable Development Goals (SDGs) adopted by the United Nations in 2015 further obligates countries to work towards ending all forms of abuse, exploitation and violence affecting children and young people by 2030. This includes any kind of abuse and exploitation faced by children and young people online. Further the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, adopted in 2007 (also known as the Lanzarote Convention) focuses on preventing, protecting and prosecuting the sexual exploitation and abuse of children. It strongly criminalises of all kinds of sexual offences against children including child pornography. In addition, the African Union has adopted the Africa Cyber Security Convention in 2014, which highlights ways to address child pornography in the region.

1 For more details see, WSIS+10 High Level Event Outcome Documents available at http://www.itu.int/net/wsis/implementation/2014/forum/inc/doc/outcome/362828V2E.pdf

It is usually a given[2] that in general, we know where our children are each day, who they are with, and what they are doing. But in the digital world, where even our youngest children are spending a growing amount of time, we are often reduced to the role of spectator and many of us are reeling from a case of 'digital whiplash'.

Children, even very young ones, may very well understand today's technology better than educators or parents. Children today have only ever experienced a world that's cyber-filled, where technology is woven into every aspect of their lives. It informs their friendships, their education and their understanding of the world and people around them. In the meantime, we as adults are scrambling to figure out which rules to set and how to enforce them.

The trouble is, this particular subject isn't covered in the parental lesson book; that chapter hasn't been written yet and society hasn't had time to form standards.

We have a legal drinking age and a legal driving age, but there is no solid, conventional wisdom about the age at which children can safely go online by themselves or text a friend on their cell phone - or about what the parents' role should be in keeping watch on our vulnerable and often naive children during their online activities.

There is a disconcerting gap between what parents think their children know and what children actually know. On average, American teens spend about five hours a day online; while parents only think their children spend an average of three hours a day online. Nearly 10% of teens (10.3%) spend more than 10 hours a day online. Two in three teens say their parents don't need to know everything they do online. In fact, half of teens would actually change their online behaviour if they knew their parents were watching.[3] Moreover only one third of households with Internet access are protecting their children with filtering or blocking software[4].

These patterns are consistent in countries around the world:

A staggering three-quarter of Australian parents admit to having no idea what their children are up to online, a recent study reveals.[5] Even though 30% of 9-10 year olds in Australia say they've been bothered by something online, their parents are unlikely to recognise this. Only 16% of their

2 http://www.parenting.com/article/Mom/Relationships/How-to-Spy-on-Your-Child-Online (last accessed 16 November 2015)

3 http://www.mcafee.com/us/about/news/2012/q2/20120625-01.aspx (Accessed 13 November 2015)

4 http://www.guardchild.com/statistics/#sthash.lrDBAYZQ.dpuf (Accessed 14 November 2015)

5 http://www.news.com.au/technology/online/the-majority-of-parents-are-in-the-dark-about-cyber-safety/story-fnjwnfzw-1227441745412 (Accessed 15 November 2015)

parents say 'yes, something has bothered my child online'.[6]

In Korea, 97% of homes have Internet connection[7], and up to one in every ten South Korean child, between the ages 10 and 19 years is addicted to the Internet.[8]

In the UK, an estimated 5.43 million young people have experienced cyber bullying with 1.26 million subjected to extreme cyber bullying on a daily basis.[9]

In order to respond to these growing challenges, ITU, together with other stakeholders, launched COP[10] Initiative in November 2008. COP has been developed by ITU as part of its Global Cybersecurity Agenda (GCA)[11] and has been established as an international collaborative network for action to promote the online protection of children and young people worldwide, by providing guidance on safe online behaviour in conjunction with other UN agencies and partners.

The key objectives of the COP initiative are to:

- Identify the key risks and vulnerabilities to children and young people in cyberspace;
- Create awareness of the risks and issues through multiple channels;
- Develop practical tools to help governments, organizations and educators minimize risk;
- Share knowledge and experience while facilitating international strategic partnerships to define and implement concrete initiatives.

These Guidelines have been prepared within the ITU's Child Online Protection (COP) Initiative and aim to provide information, advice and safety tips for parents, guardians and educators on child online protection.

6 CCI, Risks and safety for Australian children on the Internet, Available at https://www.ecu.edu.au/__data/assets/pdf_file/0009/294813/U-Kids-Online-Survey.pdf (Accessed 15 November 2015)

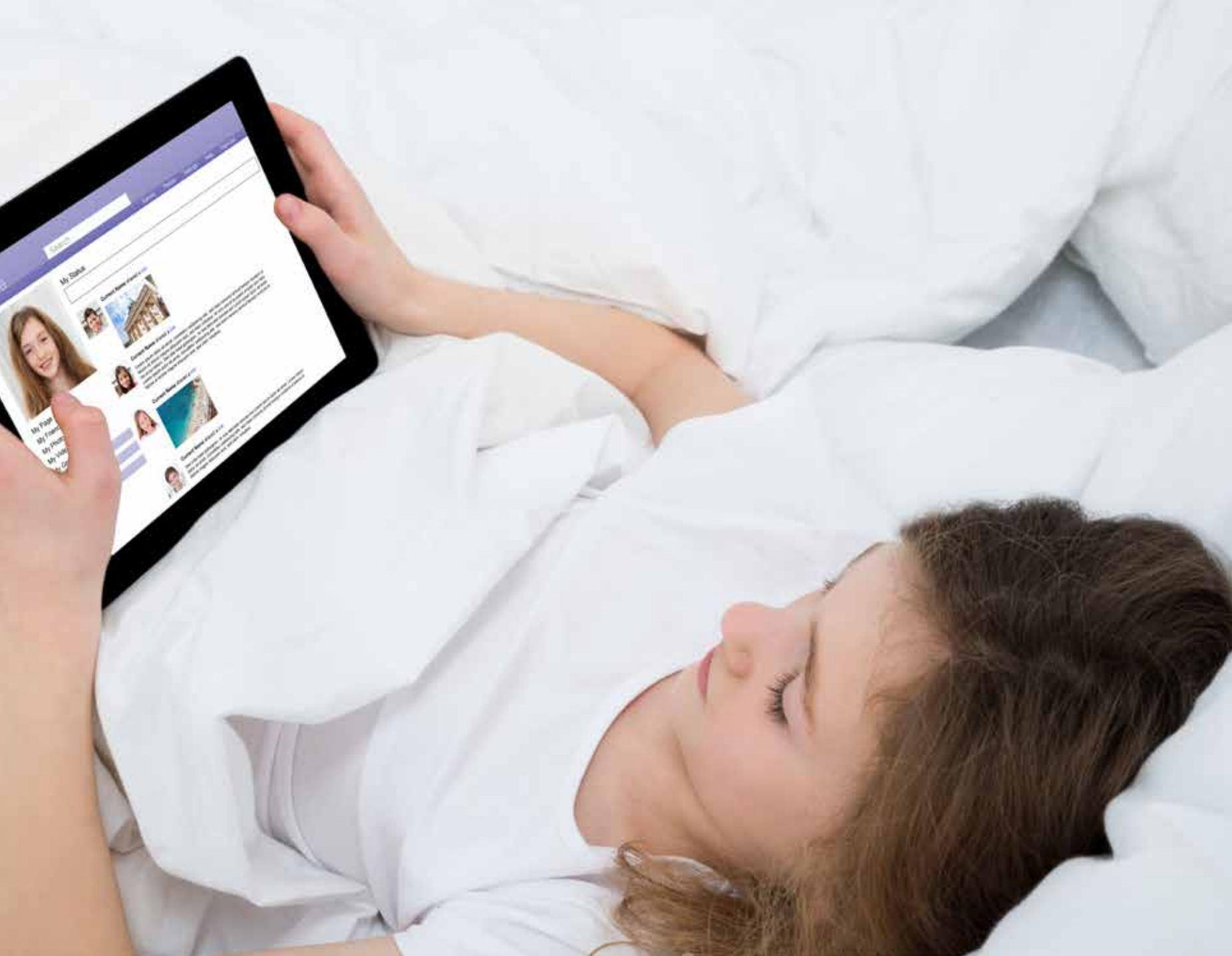
7 Pacific Telecommunications Council, Broadband Policy in South Korea, http://www.ptc.org/ptc12/images/papers/upload/PTC12_Broadband%20Policy%20Wkshop_Jamie%20Ahn.pdf (Accessed 13 November 2015)

8 http://www.abc.net.au/news/2015-09-13/south-korean-children-seek-help-at-digital-detox-boot-camp/6769766 (Accessed 13 November 2015)

9 http://www.ditchthelabel.org/the-cyber-bullying-survey-2013/ (Accessed 13 November 2015)

10 www.itu.int/cop

11 www.itu.int/osg/csd/gca


My Status

2. Children and Young People Online

The Internet has continued to change dramatically in recent years. Social networking sites (e.g. Facebook), micro-blogging (e.g. Twitter), blogs (e.g. Wordpress), media sharing (e.g. YouTube, Instagram, Flicker, Snapchat), online encyclopaedias (e.g. Wikipedia), podcasting (e.g. blogtalkradio), social voting (e.g. digg), social bookmarking (e.g. delicious) online games and virtual worlds have increased the Internet's connectivity, encouraging online social connections and allowing surfers to create their own content. In 2016, it is estimated that there will be around 2.13 billion social network users around the globe, up from 1.4 billion in 2012.[12] At the end of 2014, there were 31% more bloggers than there were three years ago[13]. The use of social networking and media sharing websites such as Facebook, Twitter, Instagram and YouTube is multiplying year after year; and communication between web users has become one of the largest source of Internet traffic.

According to a pan European survey in 2014[14], children and young people (aged 11 to 16 years) use ICTs mostly to engage in social networking, instant messaging, to watch video

12 http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (Accessed 13 November 2015)

13 http://aci.info/2014/12/27/the-state-of-blogging-in-2014/ (Accessed 13 November 2015)

14 http://lsedesignunit.com/EUKidsOnline/index.html?r=64 (Accessed 13 November 2015)

Type of player	Interested in	Likely to be	Characteristics
Explorer-investigators	Following a quest, solving a mystery, going on a journey, being 'outdoors'	The more confident children, no age or gender difference	Examines the detail, curious and communicative, imaginative engagement with the mystery
Self-stampers	Presenting themselves in the world	Both genders, possibly more older children	Boys and girls want to 'make their mark' on their avatar, perhaps with their own face; older girls want to dress-up and make up their avatars. Both boys and girls want to express themselves through the creation of a home or "base".
Social climbers	Ranking, social position within the environment	Both younger and older children; only some gender bias (boys slightly more than girls)	Competitive; concerned with ranking and exhibiting that ranking to others
Fighters	Death and destruction, violence, and superpowers	Male, slight bias towards older boys	Children express frustration when not having a means to express themselves; offering opportunities to "win" and "defeat opponents" lessens the frustration.

Type of player	Interested in	Likely to be	Characteristics
Collector-consumer	Accumulating anything of perceived value within the system	Older boys and girls	Collects pages and coins, seeks shops, gift-giving opportunities, an economy and a place to put belongings
Power users	Giving everyone the benefit of their knowledge and experience	Expert in the games, the geography of the environment, the systems	Spend several hours at a time playing and exploring the game, with a deep interest in how the game works
Life-system builders	Creating new lands, new elements to the environment, populating the environment	Younger children (imagined worlds without any rules), and older children (imagined worlds with rules and systems – houses, schools, shops, transport, economy)	Children express frustration when not having a means to express themselves; systems (or lack of them) to govern the environment are appealing.
Nurturers	Looking after their avatar and pets	Younger boys and girls, and older girls	Children want to meet and play with others, to teach their avatar skills such as swimming, and to have a place for their avatar to sleep. Virtual pets are also appealing.

clips and play online games. This provides a variety of positive opportunities for participation, creativity and education. It also allows communication between young people across national, religious and cultural borders. For example the following table describes the type of online experiences the children will be most likely to have when accessing virtual worlds[15]:

The Internet is a neutral tool for disseminating data, which can be used for good or bad purposes. On the one hand for example, it has enormous potential as a source of education for people of all ages and capabilities. Whilst on the other hand, the Internet can be used to set online traps to exploit users for criminal purposes and unfortunately children are among those who are most vulnerable to such traps.

It is important to remember that the Internet is not the only communication tool, which can potentially negatively affect the wellbeing of children. In the last few years, the use of mobile phones by young people has increased dramatically, and children are using their mobile phones to access the Internet virtually anywhere they go. Smartphones as they are known, can be used for video messaging, entertainment services (downloading games, music, and videos) as well as access to the Internet and location-based services. This increases the likelihood that they will be exposed to dangers online without the supervision of an adult. A recent study in South Korea shows 72% of children own a smartphone by the age of 11 or 12 and spend on average 5.4 hours a day on them.[16]

The potential risks faced by children accessing the Internet through mobile phones or other personal devices are similar to those where the Internet is accessed via a wired connection. The big difference between accessing the Internet through a child's mobile phone, laptop or tablet compared to traditional access through a home computer is the very private nature of such mobile personal devices. Where personal devices are used primarily by teenagers typically parents cannot use direct supervision in the same way as they would on a computer at home. Parents should talk to their children regarding usage and ensure that they enable controls on children's devices when they are purchased or used for the first time.

15 ENISA, Children on virtual worlds - What parents should know, September 2008, available at https://www.enisa.europa.eu/publications/archive/children-on-virtual-worlds (Accessed 16 November 2015)

16 http://www.bbc.com/news/world-asia-33130567 (Accessed 13 November 2015)

Case Study: Egyptian Young People and the Internet

The Egyptian Youth Internet Safety Focus Group (Net-Aman) consists of 11 members aged 18 to 28, and is an integral part of the wider Cyber Peace Initiative developed by the Suzanne Mubarak Women's International Peace Movement with support from a range of partners.

The name of the focus group is Net-Aman ("net-safety" in Arabic) has been picked out by all the youth members. The mandate of this group is to increase awareness about Internet safety and the huge potential of ICT with the aim to offer children and youth the chance to identify by themselves harmful content and decide on the best way to deal with that through a participatory approach.

The initial training session of Net-Aman has produced a questionnaire that the members used to capture a "snapshot" of children and youth's concerns and hopes about using the Internet in Egypt. Each youth was commissioned to go into schools and universities, and submit a report on the findings of the survey in the second training session in March 2008. The survey represented diversified age group of young people, including from 8 to 22 years. This survey helped Net-Aman to understand what young people in Egypt feel about the Internet and their safety.

Approximately 800 Egyptian young people responded to the youth2youth survey entitled "Egyptian young people and the Internet".

The children and young people surveyed asserted that:

- They are not monitored by any adults while using the Internet.
- Concerning the risks and challenges of the Internet in Egypt, they listed: The main online risk is inappropriate content, followed by viruses and spywares, violent content, copying for homework (plagiarism), while the last risk is cyber bullying.
- One of the most shocking results of the survey that most youth are sharing their personal information, full name, age, photos, school information and phone numbers over the Internet without any concern about the consequences.

In light of the results of this survey and in line with the mandate of the Egyptian Youth Internet Safety Focus Group (Net-Aman), the youth members will continue to contribute and participate in efforts that will help to raise awareness on child online protection issues for the youth of Egypt.

3. Parents, Guardians and Educators

Defining parents, guardians and educators

Several Internet sites refer to parents in a generic way (such as on a "parents page" and refer to "parental controls"), therefore, it might be useful to define the people who ideally should ensure that children use Internet sites safely and responsibly and grant their consent to have access to specific Internet sites.

In this document, the term "parents" will refer to the natural mother and/or father of a child or a person to whom guardianship has been granted.

Today's world presents a myriad of cases where people other than the natural parents may take care of children. They are often referred to as guardians or caregivers, and it is important and imperative to recognise the role

they can play while the children under their care are online.

An educator is a person who systematically works to improve another person's understanding of a topic. The role of educators encompasses both those who teach in classrooms and the more informal educators who, for example, work in Social Networking sites to provide online safety information or run community or school based courses to enable children to stay safe online.

The work of educators will vary depending on the context in which they work and the age group of the children (or adults) they seek to educate.

All those who come into contact with children and young people – parents, teachers, social care providers, library services, family support workers, youth leaders and wider members of the family including grandparents. It is important to note that children in the care of social services are a particularly vulnerable group and as such need special attention.

Also, what it is important to look at the role of peer mentoring – as these individuals will be educators in one sense of the word.

What many parents, guardians and educators don't know

Recent analysis conducted by McAfee[17] has highlighted that in most cases parents and guardians are not aware of details concerning the online experiences their children are likely to encounter and the risks and vulnerabilities related to various online activities.

Feature	Description
Build profiles	Input information about themselves.
Interact with others	Share information and ideas with other users through chat, blogs, instant messaging, discussion forums and voice over Internet protocol (VoIP) features.
Create avatar	Choose a graphic image to represent themselves and establish their identity in the Internet site.
Play games	Challenge their minds and provide activities to participate in online.
Respond to quizzes	Challenges such as brain training, generally with a reward of some kind for participation. Also, provides competition between friends or groups of friends in the form of "leaderboards".
Make drawings, animation, comic strips and gadgets	Also called UGC or User-Generated Content, many children enjoy creating their own content to share with their community, and thrive creatively when collaborating with others in their virtual community.
Create content ranging from music and dance to video	Self-publishing has opened up to all ages and can be an excellent creative outlet.
Buy products	Some services may allow users to purchase products or services using real money.
Upload photos or any other information	Some services may allow children to upload photos and information. Some will filter for personal and/or other inappropriate content.
Download music	Some services may allow children to download music.
See advertisement about products/ services	Internet sites are often supported by advertising.

17 McAfee Digital Deception Study 2013: Exploring the Online Disconnect between Parents & Pre-teens, Teens and Young Adults, Available at http://www.mcafee.com/us/resources/reports/rp-digital-deception-survey.pdf (Accessed 16 November 2015)

Children can be online using different platforms and devices which can include desktop computers, laptop computers, mobile phones, smartphones, tablets, other handheld devices such as iPod Touch, e-book readers and games consoles. Depending on the type of platform used and the features that are available, each person's experience will be different. For example young people go online for a variety of different reasons including the following[18]:

Interact with friends in real time through instant messaging, message boards and chat rooms that are integrated into the sites;

- Meet known friends and make new friends;
- Create and design a personal website using graphics, colour, music and images to represent the user's unique style and identity;
- Link to friends' personal websites;
- Upload and share images of themselves, their family and friends;
- Upload and share videos;
- Create blogs, journals or diaries about their lives;
- Publish and share their own music;

18 UK Council for Child Internet Safety, Good practice guidelines for the providers of social networking and other user interactive services, updated 2010, 2010, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251456/industry_guidance_social_networking.pdf

Case Study : Privacy in peril

Many users are unaware of how much personal information they give away online or even how it is being done! Such methods include:

- Forgetting to click on privacy settings, and
- Giving away more information than is required

However, for children and young people, this leaves them vulnerable to (perhaps) inappropriate contact by a peer, older youth or even an adult. Children may also innocently give away information about themselves by:

- Completing any type of form (e.g. contest and registration)
- Posting personal profiles
- Building a website

It is important for parents not to exaggerate the risks or to frighten children unduly in the way we discuss the risks they may encounter online.

Knowing how children can innocently give out information online, and how easily strangers can find information about them, is one of the important things to be taken into consideration.

Children need to know there are many databases that are able to provide information about their address, phone number and e-mail address. Children and young people should be encouraged to use privacy settings at all times whilst online and to alert a responsible adult if they are asked for personal (physical) information or are uneasy about their online communication.

Below is a mock chat room discussion that law-enforcement officers believe to be a realistic example of online discussions. Imagine a predatory paedophile sitting and taking notes on this child, and using this information to lure them later. Would your child fall for this?

Unfortunately some would.

Child: I hate my mom! I know it's her fault that my parents are getting divorced.

Predator: I know. My parents are getting divorced, too.

Child: We never have any money anymore, either. Every time I need something, she says the same thing: "We can't afford it." When my parents were together, I could buy things. Now I can't.

Predator: Me too. I hate that!

Child: I waited for six months for the new computer game to come out. My mom promised to buy it for me when it came out. She promised! Now it's out. Can I buy it? Nope. "We don't have enough money!" I hate my mom!

Predator: Oh! I'm so sorry! I got it! I have this really kewl uncle who buys me things all the time. He's really rich.

Child: You're sooooo lucky. I wish I had a rich and kewl uncle.

Predator: Hey! I got an idea! I'll ask my uncle if he'll buy you one too....I told you he's really kewl. I bet he'd say yes.

Child: Really!? Thanks!!

Predator: BRB [cybertalk for "be

right back"] . . . I'll go and call him.

Predator: Guess what? He said okay. He's gonna buy you the game!

Child: Wow, really? Thanks. I can't believe it!!!

Predator: Where do you live?

Child: I live in NJ. What about you?

Predator: I live in New York. So does my uncle. New Jersey isn't far.

Child: Great!

Predator: Is there a mall near you? We can meet there.

Child: O.K.. I live near the GSP Mall.

Predator: I've heard of that. No prob. What about Saturday?

Child: Kewl.

Predator: We can go to McDonald's too if you want. We'll meet you there at noon.

Child: O.K.. Where?

Predator: In front of the computer game store. Oh! My uncle's name is George. He's really kewl.

Child: Great . . . thanks, I really appreciate it. You're so lucky to have a rich and kewl uncle.

Child: Really!? Thanks!!

Predator: BRB [cybertalk for "be right back"] . . . I'll go and call him.

Predator: Guess what? He said okay. He's gonna buy you the game!

Child: Wow, really? Thanks. I can't believe it!!!

Predator: Where do you live?

Child: I live in NJ. What about you?

Predator: I live in New York. So does my uncle. New Jersey isn't far.

Child: Great!

Predator: Is there a mall near you? We can meet there.

Child: O.K.. I live near the GSP Mall.

Predator: I've heard of that. No prob. What about Saturday?

Child: Kewl.

Predator: We can go to McDonald's too if you want. We'll meet you there at noon.

Child: O.K.. Where?

Predator: In front of the computer game store. Oh! My uncle's name is George. He's really kewl.

Child: Great . . . thanks, I really appreciate it. You're so lucky to have a rich and kewl uncle.

Saturday arrives, and the child goes to the mall and meets an adult outside the computer game store. He identifies himself as "Uncle George" and explains that his nephew is already at the McDonald's waiting for them.

The child is uncomfortable, but the uncle walks into the store and buys the $100 game. He comes out and hands it to the child, who is immediately neutralized and delighted.

Stranger-danger warnings are not applicable. This isn't a stranger- he's "Uncle George," and if any proof was needed, the computer game is it. He gets into Uncle George's car without hesitation to meet his friend at McDonald's. The rest is reported on the 6 o'clock news.

It's disgusting. It makes us sick to our stomachs, but it happens. Not very often, but often enough that you need to be forewarned. (Several hundred cyberpredators are caught and arrested each year.) Even once is too much, though, if it's your child. Knowing how they operate and the tricks of the trade will help you teach your child. how to avoid being victimized.

Source: http://www.wiredkids.org/parents/parry_guide.html

- Share thoughts and information on areas of interest;
- Play online games;
- Receive comments or messages on their personal websites from friends or guests; create or join wider communities or interest groups, e.g. football or music; and
- Complete or create questionnaires integrated into some social networking sites.

Even if the user experience is different when an Internet site is accessed through a smartphone rather than through a personal computer, the risks and vulnerabilities related to the use of the Internet are the same regardless of the platform. Parents and guardians have misconceptions, often saying that they would rather their children were at home using a computer rather than being outside and not knowing where they are. Of course the Internet can take children and young people anywhere and they can be exposed to risks in the same way as they can in the real world. (See case study ahead)

Online risks and vulnerabilities related to the use of the Internet for children and young people

- Exposure to illegal and harmful content, such as pornography, gambling, self-harm sites and other content inappropriate for children and contact with other users. In most cases, operators of these sites do not take effective measures to restrict access of children to their websites.
- Creation, reception and dissemination of illegal and harmful content.
- Pretending to be someone else, often another child, as part of a deliberate attempt to harm, harass or bully someone else.
- Undesirable contact, especially with adult impostors posing as children.
- Disclosure of personal information leading to the risk of physical harm.
- Criminal attempts to impersonate Internet users, primarily for financial gain. In some instances this might include identity theft, although this is normally associated with attempts to defraud adults.
- Physical harm through real-life encounters with online acquaintances, with the possibility of physical and sexual abuse.
- Targeting through spam and advertisements from companies using Internet sites to promote age and/or interest-targeted products.
- Compulsive and excessive use of the Internet and/or online gaming, to the detriment of social and/or outdoor

activities important for health, confidence building, social development and general well-being.

- Bullying and harassment.
- Self-harm, destructive and violent behaviours such as "happy slapping".
- Exposure to radicalisation and racism and other discriminatory speech and images.
- Defamation and damage to reputation.
- Infringement of their own or the rights of others through plagiarism and uploading of content (especially photos) without permission. Taking and uploading inappropriate photos without permission has been demonstrated to be harmful to others.
- Infringement of other people's copyright e.g. by downloading music, films or TV programmes that ought to be paid for.
- Relying upon or using inaccurate or incomplete information found online, or information from an unknown or unreliable source.
- Unauthorised use of credit cards: the credit cards of parents or others which can be used to pay for membership fees, other service fees and merchandise.
- Misrepresentation of a person's age: either a child pretending to be older so as to gain access to age inappropriate sites, or by an older person for the same reason.
- Use of parent's email account without consent: when parental consent is required to activate an account in virtual world sites for children, children may abuse access to the accounts of their parents. Some services accounts can be difficult for parents to delete once been activated.
- Unwanted advertising: some companies spam children through virtual world sites to sell products. This raises the issue of user consent and how this should be obtained. There is insufficient legislation in this area and it is clearly very difficult to determine when children are able to understand data transactions. Indeed how to apply these rules on the Internet is already a major concern, and mobile phone access accentuates the problem.

•

Especially, the following present the greatest concerns for educators as they often feel ill-equipped to deal with them:

- Social networking – the way in which children and young people live their lives using social spaces is very different from anything that many educators are familiar with. Many cannot understand why it is so important to have so many "friends" on a contact list, but the number of friends is seen to equate to popularity for younger users. A typical teen Facebook user has an average of 300 friends while the typical teen Twitter user has 79 followers found a study in the United States.[19]
- Sexting – the relatively new phenomenon where children and young people are putting themselves at risk by posting sexually provocative images of themselves online or sending them to friends using mobile technologies.

How children are using new media – as opposed to how we think they are – There is some good research available (in individual countries) that can help to support this work. (Also, see EU Kids Online for summaries of EU issues, risks etc. at www.eukidsonline.net).

Where to go for help? Many countries have helplines where children and young people can report a problem. These are widely publicised and different countries have different approaches to getting this message out. It is important that children and young people realise that it is never too late to report a problem and that by doing so they may help others.

How educators might be at risk from bullying (e.g. children and young people who create hate sites about teachers or other professionals). Educators need to feel confident that they can use the technology safely. Many

19 http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/ (Accessed 19 November 2015)

educators feel ill-equipped to deal with some of these issues and are uncertain about how to actually have material removed from sites etc. The teachtoday website (www.teachtoday.eu) provides some excellent guidance around this and other related subjects.

It is important to emphasise (as mentioned above), that although some educators may not be as technically proficient at using the technologies as children and young people, they are well equipped in life skills and experience to be able to offer advice, guidance and support. This needs to be reiterated to educators when providing training on e-safety issues.

A recent study by the Brookings Institution[20] notes that when teens were asked what being safe online entails, 25% mentioned issues of privacy and "ensuring no one has access to personal or identifying information."17% of youth "say safety means preventing harm or harassment." The biggest concern among parents regarding youth online safety was "avoiding 'stranger danger' scenarios,"' followed closely by protecting teens' privacy and personal information.

While children acknowledge that they sometimes allow themselves to engage in risky behaviour, they do not show a lot of anxiety about the inherent risks of this type of behaviour and show a preference for trying to solve the problems by themselves or within their peer group. This suggests that they turn to their parents or other adults only in cases of potentially 'dramatic' problems. This is a problem particularly with older boys who may be more likely to use a 'Report Abuse' button[21] (such as developed by the Virtual Global Task Force). However, this is not the case with all children. We can see that children who are aware of risks, do 'police' their own activities but often do not share a view of the new technologies that implies that adults should be the reference point for judging and monitoring young people's behaviour.[22] We need to be cautious about making simple distinctions between offline and online worlds, as this no longer captures how our everyday lives have become increasingly associated with online technologies. For many children this means a careful negotiation

20 Farrukh, A., Sadwick, R., & Villasenor, J., Youth Internet Safety: Risks, Responses, and Research Recommendations, Brookings Institution, 2014, Available at http://www.brookings.edu/~/media/research/files/papers/2014/10/21-youth-internet-safety-farrukh-sadwick-villasenor/youth-internet-safety_v07.pdf

21 http://www.virtualglobaltaskforce.com/

22 Quayle, E., Lööf, L. & Palmer, T. Child Pornography and Sexual Exploitation Of Children Online. Bangkok: ECPAT International, 2008.

between the opportunities that technology offers (such as exploring their identity, establishing close relationships and increased sociability) and risks (regarding privacy, misunderstandings and abusive practices) afforded by internet-mediated communication.[23]

Same role for everyone?

It is important to remember that for children and young people, it is the teachers and parents who are the primary supports for learning[24]. The UK Byron Report[25] suggests that child protection policies should include an Awareness-Raising Campaign, which supports the learning of adults (parents, teachers, guardians) who may not be familiar with technology, as well as empowering children in terms of encouraging safety considerations and less risk taking.

The right messages for the right people

The main objective of such a campaign is to change behaviour, including encouraging safer online behaviours by children, encouraging effective online parenting by parents and encouraging others who interact with children (extended family members, teachers, etc.) to teach children to stay safe online.

Children's Internet safety should not be looked at as an isolated issue but rather as one, which has commonalities within a range of initiatives concerning children, their safety and the Internet.

The role parents and guardians can play

To ensure that children use Internet sites safely and responsibly, parents and guardians can:

1. Talk to their children about what they do and who they communicate with when they use their computer, or personal device, such as a mobile phone or games console. Opening and maintaining this dialogue is crucial to helping to keep children safe.
2. Read the terms and conditions of use with their children before they enter the site, discuss safety precautions together, set some basic rules and monitor use to ensure that the rules are respected.
3. Educate young users about responsible use of technology in general, encouraging them to listen to their instincts and use their common sense.

23 Livingstone, S. Taking risky opportunities in youthful content creation: teenager's use of social networking sites for intimacy, privacy and self-expression. New Media and Society, 10 (3), 2008, 393-411.

24 Livingstone, S., Bober, M. UK Children Go Online, Final report of key project ndings, April 2005

25 Byron, T., Safer Children in a Digital World, 2008.

4. Check to see if the site uses technical solutions such as:

   • Filters and parental controls.

   • Maintains user history.

   • Moderation, if so is it carried out by humans or by automated means e.g. using text filtering which will recognise specific words patterns and URLs? Does the site use a combination of human intervention and technical tools? Human moderators are trained to ensure a safe and appropriate environment. Active moderators are often portrayed as characters or participants in the virtual world or, in a gaming context, may act as an in-game host, in each case they are visible to all users. Usually an in-game moderator will intervene only when difficult situations occur, but in some games they will assist users who appear to be "lost" or in need of assistance. Silent moderators usually stay in the background blocking offensive material, reacting to suspicious behaviour, warning users, and performing other policing activities.

   • If the site allows photographs or videos to be posted does the site actively moderate these or does it only review images following the receipt of a report?

   • Reporting and blocking functionalities: usually tools to report inappropriate postings, conversations and activities are available, such as " flagging" and "report buttons". The virtual world should also display a clear policy on how to report inappropriate behaviour and to whom. Children should be taught how to report incidents or unwanted contacts and how to block unwanted contacts, use privacy settings and record online conversations.

   • Ratings: parents and guardians should be aware of rating symbols and their use as an important tool to protect young users from inappropriate services and content.

   • Age verification: if a site claims to use age verification, how robust are its systems? If age restricted products are on sale is a reliable age verification system used to confirm the person's age?

5. Stay involved in online young users' activities. It is crucial to

underscore the importance of the role parents and caregivers can and should play within Internet sites because their involvement has a powerful effect on their children's experience, promoting positive behaviour.

6. Stay calm and don't jump to conclusions if you hear or see anything that concerns you about your child's behaviour or the behaviour of one of their online friends. Some Internet sites are social lifelines for some young people. If your children fear that you will simply cut off their social lifeline, they are likely to be increasingly reluctant to share problems or concerns that they may have.
7. Be aware that your child may behave quite differently online than offline, face to face with you. It is not unusual for people to be more aggressive online, where they don't think anyone will hold them accountable. Use any reports of inappropriate behaviour by your child as an opportunity to discuss with your child the appropriate tone of communications online.
8. Learn the online culture so you can assess the authenticity of the typical excuses young people give when faced with accountability for their behaviour online, such as "someone stole my account". This is rarely the case when it comes to messages and chat logs, which have violated a virtual world's rules. It can happen, but it is exceptional.
9. Teach your children not to share their access passwords with friends or siblings. This is one of the biggest problems Internet sites face with young people. For example, a best friend of a sibling can steal virtual items that your child has worked hard to collect.
10. Use the website contact page to share your concerns and questions. It is their job to make sure you feel comfortable with the site.
11. Don't assume everyone on the Internet is targeting your child. Statistics show that offline problems with paedophiles far outweigh online incidents. In general, children's sites can be safe and can provide a wonderful, creative social and educational experience for your child, but only if you stay involved and aware.

The role educators can play

It is very important that educators do not make any assumption about what children and young people may or may not know about e-safety issues. There are many misconceptions about the Internet and what either is, or is not appropriate. For example many teenagers share passwords with each other and this is often seen as a sign of true friendship. An important role for educators

is to teach children and young people about the importance of passwords, how to keep them safe and how to create a strong password.

Similarly, with regard to issues of copyright, many adults are horrified at the apparent lack of concern that younger users have about downloading illegal music and video. Research[26] suggests that rather than not caring about copyright, children and young people are hugely lacking in knowledge regarding issues of legality concerning copyrighted content online. Again, there is a clear role for educators to play here in explaining this to pupils.

Schools have the opportunity to transform education and help pupils to fulfil both their potential and to raise standards with ICT's. However it is also important that children learn how to be safe when they are using these new technologies, particularly Web 2.0 collaborative technologies such as social networking sites, which are becoming an essential aspect of productive and creative social learning.

Educators can help children use technology wisely and safely by[27]:

- Making sure that the school has a set of robust policies and practices and that their effectiveness is reviewed and evaluated on a regular basis.
- Ensuring that everyone is aware of the acceptable use policy (AUP) and its use. It is important to have an AUP, which should be age-appropriate.
- Checking that the school's anti-bullying policy includes references to bullying over the Internet and via mobile phones or other devices and that there are effective sanctions in place for breaching the policy.
- Appointing an e-safety coordinator.
- Making sure that the school network is safe and secure.
- Ensuring that an accredited Internet service provider is used.
- Using a filtering/monitoring product.
- Delivering e-safety education to all children and specifying where, how and when it will be delivered.
- Making sure that all staff (including support staff) have been adequately trained and that their training is updated on a regular basis.
- Having a single point of contact in the school. And being able to collect and record e-safety incidents which will give the school a better

26 Berkman Center, John Palfrey and Urs Gasser, 2008

27 BECTA. Safeguarding Children Online. 2009.

picture of any issues or trends which need to be addressed.

- Ensuring that the management team and school governors have an adequate awareness of the issue of e-safety.
- Having a regular audit of all e-safety measures.
- Educational and psychological effects
- Children's use of Internet technology has risen dramatically in recent years and has been accompanied by a growing concern about issues of online safety. Throughout history there has been a recurring moral panic about the potential danger of

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/ hateful content	Pornographic or unwelcome sexual content	Bias, racist or misleading info or advice
Contact (child as participant)	Tracking/ harvesting personal info	Being bullied, harassed or stalked	Meeting strangers, or being groomed	Self-harm or unwelcome persuasions
Conduct (child as actor)	Illegal, downloading, hacking, gambling, financial scams or terrorism	Bullying or harassing another person	Creating and uploading inappropriate material	Providing misleading information/ advice

Table developed by the EUKids Online project and referenced in paragraph 1.3 of the Byron Review.

communication technologies and this has particularly been the case for young women. However, it has been argued that when such dangers are actually investigated it appears that very often it is not the technology as such that is the culprit but more the agency of the children using the technology and the anxieties about loss of parental control[28]. Educators have been perceived to have a vital role in promoting and ensuring Internet safety. Parents across the world appear to believe that schools should have a central role in educating children in safe technology use and the Children's Charities Coalition have also suggested that "Clearer guidance should be offered to schools on the safe use of Internet, emails, chat rooms, school web sites, and filtering and blocking software"[29].

- Early approaches to online safety focused largely on technological solutions, such as the use of filtering software, but more recently we have seen the increasing mobility of information technology and as a result, desktop computers are no longer the sole access point to the Internet. Presently increasing numbers of mobile phones and games consoles offer broadband connections and children can access the Internet while at school, at home, in the library, at an Internet café, a fast-food outlet, a youth club or even travelling to school on public transport. Schools offer the opportunity to work on the Internet, collaboratively within a closed network or simply surrounded by other children. Obvious measures include setting up effective security in the network but we need to go beyond this. Children may have personal devices that are not covered by network protection and BECTA (British Educational Communications and Technology Agency) have argued that the emphasis should be on getting everyone to understand the risk and act accordingly.
- They suggest that this means designing and implementing e-safety polices which demand the involvement of a wide range of interest groups. These include:
- Head teachers
- Governors
- Senior management

28 Cassell, J. & Cramer. M. High Tech or High Risk: Moral Panics about Girls Online. In T. McPherson (Ed.) Digital Youth, Innovation, and the Unexpected. The John D. and Catherine T.MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA: The MIT Press, 2008. 53–76.

29 Children_s Charities_ Coalition for Internet Safety (2001). _Working to make the Internet a safer place for kids. Available at www.communicationswhitepaper.gov.uk/pdf/responses/ccc_internet_safety.PDF

- Classroom teachers
- Support staff
- Young people and parents or caregivers
- Local authority personnel
- Internet service providers (ISPs), other electronic service providers (ESPs), such as the publishers of social networking sites, and regional broadband consortia, who are working closely with ISPs and ESPs on network security measures.

BECTA has argued that as all of these groups have insights that can help set school policies, it is important that they are all consulted. However, simply having policies is not enough and, everyone involved with children should undertake active practices that help young people and staff to identify and achieve safe behaviour. By involving all these groups from the start, everyone should feel the relevance of such policies as well as their personal responsibility for making them real.

Creating a safe ICT learning environment has several important elements, which include the following:

1. An infrastructure of whole-site awareness;
2. responsibilities, policies and procedures;
3. an effective range of technological tools;
4. a comprehensive e-safety education;
5. programme for everyone in the establishment;
6. a review process which continually monitors the effectiveness of the above[30].

These should all be embedded in existing child safety policies within the school, rather than be seen as something managed solely by an ICT team. It makes little sense to think of bullying over the Internet or via mobile phone as being something apart from bullying in the offline world.

However, this does not mean that technology cannot also be an important part of the solution through setting up:

7. Virus prevention and protection
8. Monitoring systems to keep track of who downloaded what, when it was downloaded, and which computer was used
9. Filtering and content control to minimize inappropriate content via the school network.

Clearly the problems that arise in relation to new technologies do not apply to all children and when problems do arise they depend on the age of the children using these technologies. At the end

30 BECTA. Safeguarding Children Online: A Guide for School Leaders: 2009. Available from http://webarchive.nationalarchives.gov.uk/20110130111510/http:/publications.becta.org.uk/display.cfm?resID=35298&page=1835

of 2008 the US Internet Safety Technical Taskforce produced its report 'Enhancing Child Safety & Online Technologies' which provided a useful literature review of original, published research addressing online sexual solicitation, online harassment and bullying, and exposure to problematic content[31]. Within this report it was noted that, 'There is some concern that the mainstream media amplifies these fears, rendering them disproportionate to the risks youth face."

This creates a danger that known risks will be obscured, and reduces the likelihood that society will address the factors that leads to known risks, and often inadvertently harm youth in unexpected ways. Media coverage of Internet mediated crimes against children often seem to mirror the polarized positions of professionals and academics who work in the area, with the pendulum swinging between those who feel that there is a danger of distorting the threat posed to children, and those for whom it appears that the threat has been grossly underestimated.

However, there is concern that Internet mediated technology may leave some children vulnerable and that educator, along with parents and guardians, have responsibilities with regard to this. The different ways in which children and young people may be victimized online include:

- Child solicitation or grooming.
- Exposure to problematic or illegal materials
- Exposure to a medium that might foster harmful behaviour on the part of young people
- Cyberbullying

A useful way to think about risk can be seen in the following table[32]:

Online solicitation or grooming

In the context of sexual solicitation, or grooming, we understand more about the process of victimization, in part because the research has largely involved the children themselves.

Much of this research has come from the Crimes against Children Research Center (CCRC) at the jUniversity of New Hampshire and has been generated by three

31 ISTTF (2008). Enhancing Child Safety and On-line Technologies: Final Report of the Internet Safety Technical Task Force To the Multi-State Working Group on Social Networking of State Attorneys General of the United States. Harvard University: The Berkman Center for Internet and Society.

32 Table developed by the EUKids Online project and referenced in paragraph 1.3 of the Byron Review.

Youth Internet Safety Surveys (YISS) namely YISS-1[33], YISS-2[34] and YISS-3[35]. These surveys involved telephone interviews with national samples of Internet users ages 10 to 17 conducted in 2000, 2005 and 2010 respectively. There are also further references to this issue in the International Youth Advisory Council Global Online Survey[36].

A US research on Internet-initiated sex crimes makes it clear that the stereotype of the Internet child molester who uses trickery and violence to assault children is largely inaccurate[37]. Most Internet-initiated sex crimes involve adult men who use the Internet to meet and seduce underage adolescents into sexual encounters.

The research further states that in the great majority of cases, victims are aware they are conversing online with adults.

However the attention has been on children being made the focus of abusive practices, ignoring the kinds of social and cultural worlds young people are creating online. Children and adolescents are not simply the targets of adult Internet creations, but are active participants in creating their own cyber cultures.

The studies from the University of New Hampshire emphasise that it is these aspects of the Internet that create risks for some young people who engage in specific behaviours with the new technologies. While the majority of youth appear to take risks (and in particular older, male children), the vast majority of children do not appear to be at risk[38]. However, young people who send personal information (e.g., name, telephone number, pictures) to strangers or talk online to such people about sex are more likely to receive aggressive sexual

33 Finkelhor, D., Mitchell, K. and Wolak, J. Online victimization: A report on the nation's youth. (NCMEC 6-00-020). Alexandria, VA: National Center for Missing and Exploited Children. 2000.

34 Wolak, J. Mitchell, K. and Finkelhor, D. Online victimization: 5 year later (NCMEC 07-06-025). Alexandria, VA: National Center for Missing and Exploited Children. 2006.

35 Mitchell, K.J., Jones, L.M., Finkelhor, D. & Wolak, J. Trends in Unwanted Online Experiences and Sexting: Final Report. 2014. Durham, NH: Crimes against Children Research Center, Available at http://scholars.unh.edu/cgi/viewcontent.cgi?article=1048&context=ccrc (Accessed 15 November 2015)

36 http://www.iyac.net/children/index.htm

37 Wolak, J., Finkelhor, D., Mitchell, K.J., and Ybarra, M.L. Online "predators" and their victims. American Psychologist, 63 (2), 2008, 111-128.

38 OPTEM. Safer Internet for Children. Qualitative Study in 29 European Centres. Brussels: European Commission. 2007. Available at http://ec.europa.eu/public_opinion/archives/quali/ql_safer_internet_summary.pdf (Accessed 16 November 2015)

solicitations, involving actual or attempted offline contact.

Following the YISSs, over a decade there was a continued decline in reports of unwanted sexual solicitations – from 19% in 2000 to 13% in 2005 and 9% in 2010. Most of the solicitors in 2000 and 2005 were people the youth met online, less so in 2010. However there was continued increase in online harassment – from 6% in 2000, to 9% in 2005 and 11% in 2010. The authors felt that this increase in harassment was largely explained by the increase in the amount of Internet use of the previous five years.

YISS-3 also note that girls are more likely to be victims of online harassment usually in the form of being called mean names, exclusion, rumours spread about them, and being made fun of or teased. There was a large increase in the proportion of female victims, rising from 48% to 69%. In fact, rates for males calculated separately did not rise during the decade.

A European study[39] highlights that the anonymity, availability of extremely sensitive personal information and ease of

39 European Online Grooming Project, Online Abuse: Literature Review and Policy Context Available at http://www.europeanonlinegroomingproject.com/media/2080/eogp-literature-review.pdf (Accessed 15 November 2015)


“The Internet can take children and young people virtually anywhere in the world – and in the process they can be exposed to potentially dangerous risks”

contacting people, makes social networking sites a useful tool for online child sex offenders in general, but specifically for online groomers. Not only a large number of children and young people are using social networking sites today, many children at younger ages have open access to such sites. Once in contact with a child, online groomers can use various incentives to encourage the child's participation, towards the goal of sexual contact. Further, the New Hampshire studies reveal in 2010, the overwhelming majority of online harassment incidents (82%) and most sexual solicitations were occurring on social networking sites, compared to pre-dominantly chat rooms in 2000.

In addition, YISS-3 notes that aggressive solicitations decreased slightly between 2005 and 2010 – from 4% to 3%. The identified risk factors for such aggressive solicitations included being female, using chat rooms, using the mobile Internet, talking with people they first met online, sending personal information to people they first met online, and experiencing offline physical or sexual abuse.[40]

In YISS-3, many solicitors (45% of all cases) wanted sexual pictures of the young person – most young people did not send a sexual picture. Being female, of African–American ethnicity, having a close online relationship, engaging in sexual behaviour online and experiencing sexual or physical abuse off-line are some of the identified risk factors for receiving a request for a sexual picture. Of interest is the fact that requests were more likely to occur when young people were with friends, communicating with an adult, someone they had met first online, who had sent a sexual picture to the young person, and who attempted or actually made, some form of offline contact[41].

In the first survey sexual solicitation appeared to be associated with showing signs of depression[42]. Young people who reported major depressive-like symptoms were 3.5 times more likely to report an unwanted online sexual solicitation compared to those with mild or no symptoms, and those with symptoms were twice as likely to report feeling emotionally distressed by the incident. In

40 Mitchell, K.J., Finkelhor, D. and Wolak, J. Youth Internet users at risk for the most serious online solicitations. American Journal of Preventive Medicine, 32 (6), 2007, S32-S37.

41 Ibid

42 Ybarra, M.L., Leaf, P.J. and Diener-West, M. Sex differences in youth-reported depressive symptomatol ogy and unwanted Internet sexual solicitation. Journal of Medical Internet Research, 6 (1), 2001, 9-18.

general, distress was more common among younger youth, those who received aggressive solicitations and those who were solicited on a computer away from their home[43].

Accounts from victims of solicitation or grooming in Sweden, both confirmed and disconfirmed the findings of the New Hampshire study. In one major Swedish case involving more than 100 girls it was evident that all of the girls knew they were meeting a man in order for him to have sex with them. At the same time none of the girls would admit to being fully aware of what this would imply.

Something in the chat conversations with the girls made the perpetrator aware of their vulnerabilities and gave him an opportunity to exploit these weaknesses even before he exploited the girls sexually. The vulnerabilities ranged from loneliness to suicidal thoughts. The fact that the girls went on their own account to the meetings with the perpetrator does not make them into consenting subjects[44].

It is obvious that the number of solicitations for online contacts is significant and that adolescents and children do report that they happen and that all children know about it. From looking into cases where offences both online and offline have occurred, it is obvious that requests for the adolescent to send images or to engage in web camera sex often marks the start of the sexual abuse.

According to an American study, 14% of online teens blogged in 2010[45]. Blogs contain material created by Internet users and share some of the qualities of social networking sites. YISS-2 found that girls are the most common bloggers, and bloggers were more likely than other young people to post personal information online[46].

However, bloggers were not more likely to interact with people they first met online who were not known to them in person. Bloggers who did not interact were at no increased risk of sexual solicitation and posting personal information in and of itself did not increase their risk. However, bloggers were at an increased risk of online harassment, regardless of whether they interacted with others online.

The UK Children Go Online Survey also suggested that young people who were less satisfied with their lives and who have become more frequent and skilled Internet users are more likely to value the Internet as a communicative environment,

43 Mitchell, K.J., Finkelhor, D. and Wolak, J. Risk factors for and impact of online sexual solicitation of youth. JAMA, 285 (23), 2001, 3011-3014.

44 Wagner, K: Alexandramannen. Förlags AB Weinco. Västra Frölunda. 2008.

45 http://www.pewinternet.org/2010/02/03/social-media-and-young-adults/

46 Mitchell, K.J., Wolak, J. and Finkelhor, D. Are blogs putting youth at risk for online sexual solicitation or harassment? Chid Abuse and Neglect, 32, 2008, 277-294.

which may lead to more risky behaviours[47].

Through practice and experience, it is possible to highlight a number of factors that need to change if we are going to be able to assist those children who have been groomed online for sexual abuse offline.

We have learnt that grooming online, as opposed to offline, happens more quickly and may be anonymous: children establish a quicker trust with their online "friend" and tend to be less inhibited in what they communicate, and such offenders are not restricted by time or accessibility as they would be in the "real" world.

In general perpetrators find out as much as they can about their potential victim; establish the risk and likelihood of the child telling; and out about the child's social networks; may give false information about themselves, including false images, and, if safe enough, they will form a "relationship" with or control the child in such a way that they are able to meet the child offline[48].

Therapeutic approaches assisting children and adolescents who have been victims of offline and online exploitation are being investigated at BUP Elefanten, which is a Child

47 Livingstone, S. and Helsper, E.J. Taking risks when communicating on the Internet. The role of of ine social-psychological factors in young people's vulnerability to online risks. Information, Communication and Society, 10 (5), 2007, 618-643.

48 Palmer, T. Just One Click. London: Barnardos. 2004.

and Adolescent Psychiatric Unit that treats sexually and physically abused children in Sweden. The project has been in progress since 2006, and has involved over 100 interviews with young people, therapists, police, prosecutors and social workers.

These young people have been subjected to a variety of abuse practices including: sexual harassment; engagement in web camera sex; having their images uploaded onto the Internet; online engagement leading to off-line abuse, and children selling sex online[49].

The analysis of this interview data suggested that these young people can be divided into three descriptive groups:

- Those that were fooled and who were lured into something unexpected;
- The risk-takers, who take risks to meet emotional needs and secure attention;
- And the self-destructive, who, for example sell sex or knowingly engage in abusive relationships.

The latter group are reluctant to see themselves as 'victims', instead positioning themselves as being in control. The results of these clinical findings suggest that many of these children reject offers of help, and it is important is that practitioners do not give up on these children but instead try to maintain contact with them until they feel ready to engage in methods of help or intervention.

One of the predominant impacts of the grooming process with children, who are made the subjects of abusive images, is to silence the children. This silence is brought about both by the fact that the young people seriously believed that the person they were going to meet was their friend and that they would not want to own up to the nature of the conversations that they held online.

The former point has implications regarding how young people define and determine friendships, the latter relates to the fact that, as alluded to above, young people become far less inhibited when communicating online.

49 Quayle, E., Lööf, L. & Palmer, T. (2008). Child Pornography And Sexual Exploitation Of Children Online. Bangkok: ECPAT International.

Accessing problematic materials online

While it would be naive to assume that pornographic or sexualized materials did not exist prior to the Internet, it is true to say that the Internet has brought with it a proliferation of easily accessible sexualized material.

While the accessibility, interactivity and anonymity of the Internet are the very factors that increase the likelihood of exposure to violent or sexual material, the New Hampshire studies also highlight the accidental exposure of young people to unwanted sexual material on the Internet. YISS-3[50] reveals approximately 1 in 4 young person who used the Internet (23%) reported an unwanted exposure to sexual material online. Most young people were exposed while they were surfing the web (68%); 32% when opening an email or clicking on a link in an email.

Virtually all exposure happened on a desktop or laptop computer (92%) mostly at home; and only 1% happened through a mobile

50 Mitchell, K.J., Jones, L.M., Finkelhor, D. & Wolak, J. Trends in Unwanted Online Experiences and Sexting: Final Report. 2014. Durham, NH: Crimes against Children Research Center, Available at http://scholars.unh.edu/cgi/viewcontent.cgi?article=1048&context=ccrc (Accessed 15 November 2015)

phone. Almost half (47%) of exposure that happened on computers in the home had software that blocked pop-up ads or SPAM email; 26% had other software that filtered, blocked or monitored how you use the Internet.

These studies also acknowledge that existing research examining the effects of such exposure to unwanted sexual material had been largely with students and young adults, rather than younger children.

It is assumed that the different kind of adolescents that are caught in abusive and exploitative relationships online may indicate that risk-takers and self-destructive young people may also be accessing pornography or visiting chat sites catering to adults searching for sex partners, there is little research to support this.

These authors also discussed the ways in which programming techniques maintained such exposure, making them difficult to get out of. The majority of children who were exposed to material regarded such exposure as not particularly distressing. However, the authors emphasised that such exposure, particularly unwanted exposure, may affect attitudes about sex, the Internet, and young people's sense of safety and community.

The YISS-3 finds that after an initial increase in unwanted exposure to sexual material between 2000 and 2005, it declined again by 2010. 24% of young people in 2000 reported unwanted exposure to sexual material; this increased to 34% in 2005, but declined again to 23% in 2010. The decrease in exposure could be due to two factors. First, spamwares and filters have been increasingly present on networks and individual computers, and their detection capacities have become more refined. Second, young people may have become better educated and more savvy about opening unidentified email or clicking unidentified links.[51]

Unexpected or partial access to material is an important issue and it has been suggested that[52]: "The newer technologies (including video but also the Internet and mobile communications) allow content to be seen out of context. One may see sets of trailers rather than the entire storyline, in which to understand the content. Editorial context has always been important in content regulation guidelines (e.g. BBFC (British Board of Film Classification), Ofcom (the communications regulator in the UK), which may prove difficult to build into parallel guidelines for new media.

However, it is clear from research on children's accidental exposure to pornography on the

51 Mitchell, K.J., Jones, L.M., Finkelhor, D. & Wolak, J. Trends in Unwanted Exposure to Sexual Material: Findings from the Youth Internet Safety Studies. Crimes against Children Research Center, available at http://www.unh.edu/ccrc/pdf/Unwanted%20Exposure%203%20of%204%20YISS%20Bulletins%20Feb%202014.pdf (Accessed 15 November 2015)

52 Livingstone, S. and Hargrave, A.M. Harmful to children? Drawing conclusions from empirical research on media effects. In U. Carlsson (ed) Regulation, Awareness, Empowerment. Young People and Harmful Media Content in the Digital Age. Göttenborg: Nordicom. 2006.

Internet that unexpected and de-contextualized content can be particularly upsetting. This poses a challenge for regulators. However, young persons' use of pornography has not been widely studied and most build on self-reports, in which differences may well be those that the prevailing societal norm would dictate to the adolescent.

Many young people are exposed to online sexual materials, and we have clearly seen that not all of that exposure is accidental or damaging. One concern is that exposure to deviant or violent pornographies may have an impact on the beliefs and attitudes of some young people, and to a lesser extent on the behaviour of a select few. This is increasingly being seen as a potential public health issue, and it would appear that the consequence of exposure in the largely unregulated medium that is the Internet certainly warrants further research[53].

Problematic opportunities

One further danger posed by new technologies relates to the media themselves and the opportunities afforded to young people to engage in ways that might be deemed worthy of concern. These might be called self-victimizing activities through both the Internet and mobile phone technology, although this term may be seen to be problematic, as it largely relates to the increasing ability to generate online content.

A recent study[54] in 2014 on children's use of mobile phones in seven European countries (Belgium, Denmark, Ireland, Italy, Portugal, Romania and the United Kingdom) and Japan reveals on average, 69 per cent of children and young people use a mobile phone. Age 10 and 12 years were the most common ages to first receive a mobile phone. Japanese children receive them at older ages (the majority at 15 years) compared to their European counterparts. On average, two in three children who use a mobile phone have a smartphone. Moreover, about 34 per cent of children surveyed use a tablet. Similarly, in the United States, a Pew Research Center says nearly three-quarters of teens have or have access to a smartphone.[55]

For many young people, the mobile phone is both a vital means of communication and a way of relating to, and participating in, an extended social world. However, there are emerging concerns that such

53 Perrin, P.C., Madanat, H.N., Barnes, M.D., Corolan, A., Clark, R.B., Ivins, N. et al. Health educationa's role in framing pornography as a public health issue: local and national strategies with international implications. Promotion and Education, 15, 2008, 11-18.

54 GSMA, NTT Docomo, Children's use of mobile phones, A special report 2014, Available at http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA_Childrens_use_of_mobile_phones_2014.pdf (Accessed 15 November 2015)

55 http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/ (Accessed 15 November 2015)

technological participation may involve practices that target other individuals or involve the young person themselves.

For example an increasingly common behaviour by teenagers is 'sexting' (sharing of sexualized images or text via mobile phones). These images and text are often shared between partners in a relationship or with potential partners, but sometimes end up being shared with much wider audiences. It is thought unlikely that young teenagers have an adequate understanding of the implications of these behaviours and the potential risks they entail.[56]

A serious concern with sexting is that young people may be creating illegal child pornography, and exposing them to possibly serious legal sanctions. Another concern is that young people may be jeopardizing their future by putting compromising, ineradicable images online that could be available to potential employers, academic institutions and family members.

In Europe, the EU Kids Online project found that 15% of 11–16 year olds had received peer-to-peer sexual messages or images. Of those, 3% said they had sent or posted such images. In the UK, 12% of 11–16 year olds Internet users had received sexual messages, with 4% sending sexual texts. A follow-up from 2010 to 2013 in five EU countries, including the UK, found an increase in young people reporting seeing sexually explicit images, in particular adolescent girls. The Child Online and Exploitation Protection Centre (CEOP) identified a marked increase in self-generated indecent images being uploaded to the Internet. In the United States, the prevalence of adolescent sexting varies widely, from 9.6% to 28%, because of inconsistencies in definition and measurement.[57]

Self-generated images or films can also be seen as part of the grooming process where the offender convinces the child

56 UNICEF, Innocenti Research Center, Child Safety Online, Global challenges and strategies, Available at http://www.unicef.org/pacificislands/ict_eng.pdf (Accessed 15 November 2015)

57 Smith, P.K., Thompson, F., Davidson, J., Cyber safety for adolescent girls: Bullying, harassment, sexting, pornography, and solicitation, Available at http://www.researchgate.net/publication/264902151_Cyber_safety_for_adolescent_girls_Bullying_harassment_sexting_pornography_and_solicitation (Accessed 15 November 2015)

to send him images of himself or herself either with clothes removed or engaging in sexual behaviour. The images are often used to persuade the child of the harmlessness in sexual contacts between a child and an adult, lowering the child's inhibition to engage in offline sex or to be paid by the adult to meet. The targeted child is vulnerable for a number of reasons such as loneliness, being bullied or in constant battles with their parents. The adolescent involved sees him or herself as an accomplice to the abuse after having sent the perpetrator images.

Bullying

We have already mentioned that bullying in the online world should not be seen as something different than what is seen in the offline environment. People sometimes refer to online bullying or bullying via mobile phone as being "cyberbullying" but this may not always help everyone understand what is actually going on.

Bullying is bullying wherever and how ever it happens. The Byron Review in the UK suggested that, 'Cyberbullying refers to bullying behaviour that takes place through electronic means such as sending threatening text messages, posting unpleasant things about people, and circulating unpleasant pictures or videos of someone."

Online bullying or bullying via mobile phone can be an extension of face-to-face bullying, or it can be a form of retaliation for offline incidents. In addition, cyberspace has become a new forum for bullying by people who might be too afraid or weak to commit bullying in traditional ways that would make them more easily identifiable. Young cyberbullies also cite the ability to preserve anonymity and reach wider audiences as reasons they began victimizing other youth online.[58]

Online bullying or bullying via mobile phone can be particularly

58 Farrukh, A., Sadwick, R., & Villasenor, J., (2014 Youth Internet Safety: Risks, Responses, and Research Recommendations, Brookings Institution, Available at http://www.brookings.edu/~/media/research/files/papers/2014/10/21-youth-internet-safety-farrukh-sadwick-villasenor/youth-internet-safety_v07.pdf

upsetting and damaging because it spreads more widely, with a greater degree of publicity and content circulated electronically can resurface at any time, which can make it harder for the victim of the bullying to get closure over the incident; it can contain damaging visual images or hurtful words; the content is available 24 hours a day; bullying by electronic means can happen 24/7 so it can invade the victim's privacy even in otherwise 'safe' places such as their home; and personal information can be manipulated, visual images altered and these then passed on to others.

Moreover, it can be carried out anonymously'.[59]

Such bullying activity can include both teasing behaviour and activity that is very aggressive and the University of New Hampshire studies have suggested that there is a big overlap between illegal acts, such as sexual harassment, and bullying.

A German study looked at victim perspectives of bullying behaviour in Internet chatrooms[60]. They identified different types of bullying which included harassment, abuse, insult, teasing, and blackmail. Such bullying was frequent and often the same children were targeted. Importantly, the study further demonstrated that there was an association between victimization experiences in school and in Internet chatrooms. Adolescents who were bullied in school were also more likely to experience chatroom victimization.

These children were also likely to be seen as less popular and with lower self-esteem and having parents who were likely to be overprotective. The study also suggested that these children moved between being victims and bullies and that this could be interpreted as "fighting back" or "letting off steam".

Victims of bullying in Internet chatrooms also reported often frequenting risky online locations and may in fact place themselves in situations in which victimization is more likely. The study indicated that, in comparison to victims of major school bullying, victims of major

59 Byron, T. (2008). Safer Children in a Digital World The Report of the Byron Review. Available at http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf (last accessed 16 November 2015)

60 Katzer, C., Fetchenhauer,D. and Belschak, F. Cyberbullying: Who Are the Victims? A Comparison of Victimization in Internet Chatrooms and Victimization in School. Journal of Media Psychology 2009; Vol. 21(1):25–36.

chat bullying more frequently exhibit socially manipulative behaviour when visiting chatrooms (for example, giving out false information about their age or sex).

Following a meta-analysis by the Cyberbullying Research Center[61] has led to the conclusion that:

1. One out of every four teens has experienced cyberbullying, and about one out of every six teens has done it to others.
2. Cyberbullying is related to low self-esteem, suicidal ideation, anger, frustration, and a variety of other emotional and psychological problems.
3. Cyberbullying is related to other issues in the 'real world' including school problems, anti-social behavior, substance use, and delinquency.
4. Traditional bullying and cyberbullying are closely related: those who are bullied at school are bullied online and those who bully at school bully online.

Further an American study finds that independent of school-based bullying, cyberbullying is associated with increased distress. Moreover youth rarely tell adults about their experiences of online bullying and do not fully capitalize on the tools provided by communication technologies to prevent future incidents[62]

61 http://cyberbullying.org/facts/ (Accessed 15 November 2015)

62 JUVONEN, J. & Gross, G.F. Extending the School Grounds?—Bullying Experiences in Cyberspace. Journal of School Health, 2008, 78 (9), 496 – 505.

4. Guidelines for Parents, Guardians and Educators

The safety tips draw on analysis the data gathered and available research. This section of the paper is intended to provide, in one convenient place, guidelines to parents, guardians and educators to help them teach their children how to have a safe, positive and valuable experience while online.

Parents, guardians and educators must consider the exact nature of the different sites, and their child's understanding of the dangers and the likelihood that the parent can reduce risks, before deciding which environment is right for their child.

The Internet has great potential as a means of empowering children and young people to help and find things out for themselves. Teaching positive and responsible forms of online behaviour is a key objective.

Parents, guardians and educators			
	#	Key Areas for consideration	Description
Safety & security of your personal computer	1.	Keep the computer in a common room	Keeping the computer in a common room and being present especially when younger children are using the Internet can be very important. If you cannot be present, consider other ways of keeping a close watch on what your children are doing online, for example by using technical tools. In larger families with multiple computers there may be some practical limits which also arise if you insist on them all being in the same room at the same time, and remember as children start to get older they are anyway entitled to some privacy. As more and more children acquire laptops, and wireless networks become commonplace in private homes, it will also be more difficult to maintain a rule of this kind.
	2.	Install firewall and antivirus software	Ensure that your computer has a firewall and antivirus software installed and that it is kept up to date. Teach your children the basics of Internet security.
Rules	3.	Agree house rules about using the Internet and personal devices, giving particular attention to issues of privacy, age inappropriate places, bullying and stranger danger	As soon as children begin to use the Internet on their own, discuss and establish a list of agreed rules. These rules should include when children can use the Internet and how they should use it.
	4.	Agree rules for mobile use	As soon as children begin to use mobile phones, discuss and establish a list of agreed rules. These rules should include whether or not your children can go online using the mobile phone and how often they can use it, what kind of material they can buy or download using it, how to deal with inappropriate items, and levels of expenditure.

Parents, guardians and educators			
	#	Key Areas for consideration	Description
Parents', Guardians' and Teachers' education	5.	Parents should become familiar with the Internet sites used by their children (i.e. services and products offered by Internet sites) and have a good understanding of how children spend their time online	Evaluate the sites that children plan to use and read the privacy policy, terms of use and codes of conduct (often called "House Rules") carefully, together with any dedicated parents' page. Also, find out if the site monitors content posted on the services pages and review your child's page periodically. Check to see if any products are sold on the site.
	6.	Investigate online resources for further information about online safety and how to use the Internet in a positive way	The positive and safer use of the Internet is celebrated around the world every year. This might involve children, the local school, industry and relevant players collaborating to create greater awareness of the opportunities to promote a positive online experience. For the most up to date information on these events search online for terms like "internet safety celebration" + "country name".
	7.	Understand how children use other personal devices such as mobile phones, tablets, games consoles, e-readers, MP3 players and PDAs	Today the Internet can be accessed by several other personal devices so similar safety issues can also arise in these environments.

Parents, guardians and educators			
	#	Key Areas for consideration	Description
Internet sites features review	8.	Consider whether filtering and blocking or monitoring programmes can help support or underpin children's and young people's safe use of the internet and personal devices. If you use such software explain what it does and why you are using it to your children. Keep confidential any relevant passwords linked to these programmes.	Issues of trust and a young person's right to privacy can arise where technical tools are used, particularly monitoring programmes. In normal circumstances it is highly desirable that a parent or guardian discusses their reasons for wanting to use of this type of software, and in schools its use should also be fully explained.
	9.	Parental consent	Some countries e.g. Spain and the USA have laws specifying a minimum age at which a company or web site can ask a young person to provide personal information about themselves without first obtaining verifiable parental consent. In the case of Spain it is 14, in the case of the USA it is 13. In other countries it is considered to be good practice to require parental consent before asking younger persons for their personal data. Many sites which cater for younger children will ask for parental consent before allowing a new user to join. Check what the consent requirements are for the sites your children want to join or are members of.
	10.	Control use of credit cards and other payment mechanisms	Control the use of landlines or mobile phones to purchase virtual items. The temptation can be too great when children are allowed to use landlines or cell phones to buy any kind of goods or services. Also, keep your credit and debit cards secure, and do not disclose your pin numbers.
	11.	Ensure age verification is implemented when purchasing goods and services online	Usually age is not verified when purchasing merchandise, however systems are becoming available to guarantee age verification at the point of sale. In all cases, carefully track your child's spending online.

Parents, guardians and educators			
	#	Key Areas for consideration	Description
	12.	Check if the Internet site uses moderation	Ensure that the Internet site moderates conversations, ideally with both automatic filters and human monitoring. Does the site review all photographs and videos that are posted on it?
	13.	Block access to undesirable content or services	Technical tools can help you to block access to undesirable websites e.g. ones which allow un-moderated content or discussions, or to block access to undesirable services or content on mobile phones.
	14.	Check contractual flexibility	Check how to delete an account – even if this will result in the forfeit of subscription fees. If the service will not allow an account to be deleted, consider not using it, or blocking access to it. Report such inability to delete to local authorities.
	15.	Look at the service scope	Analyse the content provider's policies and their compliance, look at the content and specific services provided and be aware of technical limitations (e.g. adverts may be not clearly identified as such).
	16.	Observe advertising, and report inappropriate advertising	Keep an eye on ads, and report to your local ad council ads that: 1. Mislead by over-simplifying complex matters. 2. Encourage children to talk to strangers or go to dangerous locations. 3. Show people, in particular children, using dangerous things or being close to dangerous things. 4. Encourage unsafe emulation or dangerous practices. 5. Encourage bullying. 6. Cause moral harm and fear to children. 7. Encourage bad dietary practices. 8. Exploit a child's credibility.

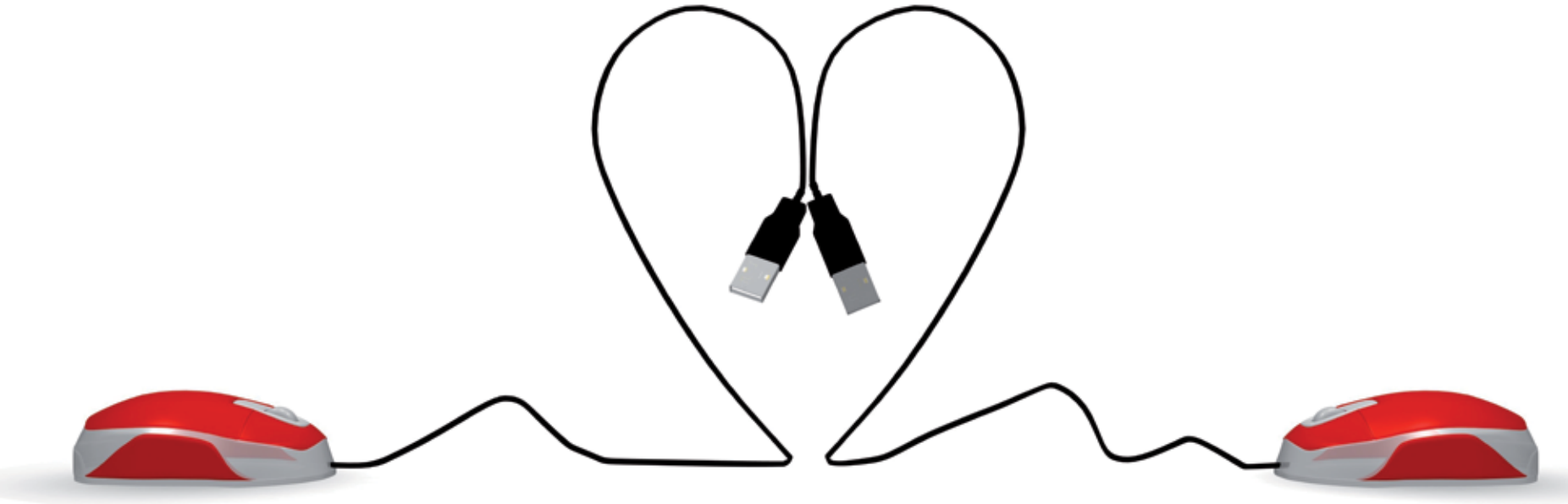
Parents, guardians and educators			
	#	Key Areas for consideration	Description
Children's educations	17.	Educate your children	Education and media literacy is crucial. Explain guidelines and rules of the virtual world. Children will likely adhere to the guidelines and often remind others to do the same. Educate your children not to reply to rude messages and to avoid sex talk online. Teach them not to open any attachment or link they receive while chatting with others because it might contain harmful content.
	18.	Explain to children to never arrange to meet in person someone they first met online	Children could be in real danger if they meet in person strangers whom they have communicated with only online. Parents should encourage children to use Internet sites only to communicate with their offline friends, not with people they've never met in person. People online may not be who they say they are. However if a strong online friendship does develop and your child wishes to arrange a meeting, rather than risk them going alone or unescorted make it clear that you would rather go with them, or ensure another trusted adult goes, and ensure the first meeting is in a public place that is well lit and has plenty of other people around.
	19.	Prevent children from sharing personally identifiable information	Help your children understand what information should be kept private. Explain that children should post only information that you – and they – are comfortable with others seeing. Remind your children that once they post information online, they cannot take it back.
	20.	Ensure children understand what it means to post photographs on the Internet, including the use of webcams	Explain to your children that photographs can reveal a lot of personal information. Children should not be allowed to use webcams or to upload any content without the approval of a parent, guardian or responsible adult. Encourage your children not to post photographs of themselves or their friends with clearly identifiable details such as street signs, license plates on cars, or the name of their school on their sweatshirts.
	21.	Warn children about expressing emotions to strangers	Children should not communicate with strangers directly online. Explain that what they write can be read by anyone with access to the same site and that predators or bullies often seek children who express an interest in making new friends online.

Parents, guardians and educators			
	#	Key Areas for consideration	Description
Internet sites safe usage review	22.	Check your child's page or profile	Check your child's page on a regular basis. Log on to view your child's account history and if necessary, change your child's chat mode to a level you are comfortable with. Well-designed Internet sites provide the opportunity for you to be deeply involved in your child's experience. If your child refuses to abide by the site's rules, you might consider contacting the site to ask for your child's pages and profile to be removed. Amongst other thing this should strengthen your message to your child about the importance of rules, and the consequences of breaking them.
	23.	Ensure children follow age limits of the Internet site	If children are under the age recommended by the Internet sites, do not let them use the sites. It is important to remember that parents cannot rely on the service provider being able to keep underage children from signing up.
	24.	Ensure children do not use full names	Wherever possible have children use nicknames – not their real names or parts of them. Nicknames should be selected carefully, such that do not attract inappropriate attention. Do not allow your children to post the full names of their friends or any other information which could be used to identify them, such as the name of the street where they live, where they go to school, their telephone number, their sports clubs, etc.
Communication	25.	Communicate with your children about their experiences	Talk to your children regularly about where they go and who they speak to when they go online. Encourage your children to tell you if something they encounter on the Internet makes them feel uncomfortable or threatened. Remind your children to stop immediately whatever they are doing when they feel uncomfortable or become suspicious. Be sure they understand they will not get in trouble for bringing something to your attention. In turn, you, as the parent and adult, should not overreact when your child shares their experience with you. Stay calm regardless of what they tell you, get all the facts, and then take action. Praise your child for trusting you. Ensure children can report abusers.

Educators[52]			
		Key Areas for consideration	**Description**
Safety & security as part of child protection strategies	1.	Use a whole-establishment approach towards responsibility for e-safety.	It is important that even if schools do not allow the use of a certain technology within the school, they teach pupils how to behave sensibly and appropriately when using it and educate them about the risks.
	2.	Develop an acceptable use policy (AUP).	These should detail the ways staff, pupils and all network users (including parents) can and cannot use ICT facilities.
Rules and policies	3.	Sample AUPs are available both online and via local authorities.	It is important to tailor these rules to fit the particular context of your establishment.
	4	Link AUPs with other school policies.	These should include policies such as anti-bullying and guidance on copyright and plagiarism.
	5.	Single point-of-contact.	Designate a senior management team member with responsibility for safeguarding to also be the central contact point for all e-safety issues.
	6.	Need for leadership.	Head teachers, supported by governors, should take the lead in embedding the agreed e-safety policies into practice.
Be inclusive	7.	Maintain awareness amongst young people.	Ensure the young people in your charge are aware of potential risks and how to practice safe, responsible behaviour, wherever and whenever they are online.
	8.	Support resiliency.	Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
	9.	Encourage disclosure of harms and responsibility taking.	Help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online

[52] BECTA (2008) Safeguarding children online. A guide for school leaders is available at: www.becta.org.uk/schools/safety

Educators[5]			
		Key Areas for consideration	**Description**
Technological solutions	10.	Audit practice.	Ensure technological measures and solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme
Internet safety policy	11.	Educate teachers on Internet safety policy.	Educate teachers on Internet safety to help and support children to be safe on the Net.
	12.	Teach students to never give out personal information when communicating with others.	Inform students that personal information (e.g., full name, address, email address, phone number, school, etc.) should never be given out when communicating with strangers online.
	13.	Require students to search for specific information only.	Require students to search for specific information, as opposed to "surfing" the Internet haphazardly and have them record, in a bibliographic format, the URLs of the sites they use.
	14.	Preview or test web sites before sending links to students.	Be sure to personally visit any site before recommending students view it. It is also a good idea to bookmark web sites ahead of time before inviting students to visit the URLs.



5. Conclusions

Information and Communication Technologies – or ICTs – have transformed modern lifestyles. They've provided us with real-time communications, borderless and almost unlimited access to information and a wide range of innovative services. At the same time, they have also created new opportunities for exploitation and abuse. Without proper safeguards, children and young people – among the heaviest users of the Internet – are at risk of unwanted sexual solicitations, harassment, and unwanted exposure to violent, sexual and other distressing material.

Without proper dedication to creating a safe cyber environment, we will fail our children. Although there is increasing awareness of the risks related to the insecure use of ICTs, there is still a significant amount of work to do. It is, therefore, crucial that parents and educators are able to decide, with their child what is appropriate and safe for their use, as well as how to behave responsibly using ICTs.

In working together, parents, educators and children can reap the benefits of ICTs, while at the same time minimizing the possible dangers for children. We hope that these guidelines will provide clear and comprehensive information on child online protection, the risks children can encounter and what parents and educators can do to protect and help their children understand how to reap the many benefits ICTs offer while minimizing potential dangers.

References and Sources for Further Reading

- 'Are ads on children's social networking sites harmless child's play or virtual insanity?', The Independent, 2 June 2008, available at http://www.commercialalert.org/news/archive/2008/06/are-ads-on-childrens-social-networking-sites-harmless-childs-play-or-virtual-insanity (Accessed 14 November 2015).
- Byron, T. (2008). Safer Children in a Digital World The Report of the Byron Review. Available at http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf (Accessed 16 November 2015)
- CCI, Risks and safety for Australian children on the Internet, Available at https://www.ecu.edu.au/__data/assets/pdf_file/0009/294813/U-Kids-Online-Survey.pdf (Accessed 15 November 2015)
- Children's Online Privacy Protection Act (COPPA) http://www.coppa.org/coppa.htm
- 'Children's social-networking sites: set your little monsters loose online', Telegraph.co.uk, 17 November 2007, available at http://www.telegraph.co.uk/technology/3355180/Childrens-social-networking-sites-set-your-little-monsters-loose-online.html (Accessed 14 November 2015).
- Child Exploitation and Online Protection Centre (CEOP): Think You Know, available at https://www.thinkuknow.co.uk (Accessed 16 November 2015).
- Cyberpeace Initiative, available at: http://www.mcit.gov.eg/Publication/Publication_Summary/144
- Cyril. A. Wantland, Subhas C. Gupta, Scott A. Klein, Safety considerations for current and future VR applications.
- Cyber-bullying: Developing policy to direct responses that are equitable and effective in addressing this special form of bullying, Canadian Journal of Educational Administration and Policy, Issue n. 57, 18 December 2006, available at https://umanitoba.ca/publications/cjeap/articles/brown_jackson_cassidy.html (Accessed 16 November 2015).
- eModeration, Virtual World and MMOG Moderation: Five techniques for creating safer environments for children, May 2008, available at http://www.emoderation.com/how-to-moderate-virtual-worlds-and-mmogs/ (Accessed 13 November 2015).
- ENISA, Children on virtual worlds - What parents should know, September 2008, available at https://www.enisa.europa.eu/publications/archive/children-on-virtual-worlds (Accessed 13 November 2015)
- Entertainment & Leisure Software Publishers Association (ELSPA), Unlimited learning –Computer and video games in the learning landscape, available at http://www.org.id.tue.nl/ifip-tc14/documents/ELSPA-report-2006.pdf (Accessed 13 November 2015)
- European Online Grooming Project, Online Abuse: Literature Review and Policy Context Available at http://www.europeanonlinegroomingproject.com/media/2080/eogp-literature-review.pdf (Accessed 15 November 2015)
- Farrukh, A., Sadwick, R., & Villasenor, J., (2014 Youth Internet Safety: Risks, Responses, and Research Recommendations, Brookings Institution, Available at http://www.brookings.edu/~/media/research/files/papers/2014/10/21-youth-internet-safety-farrukh-sadwick-villasenor/youth-internet-safety_v07.pdf

- Gauntlett, David and Lizzie Jackson, Virtual worlds – Users and producers, Case study: Adventure Rock, Communication and Media Research Institute (CAMRI), University of Westminster, UK, available at http://www.bbc.co.uk/blogs/knowledgeexchange/westminsterone.pdf (Accessed 13 November 2015)
- GSMA, NTT Docomo, Children's use of mobile phones, A special report 2014, Available at http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA_Childrens_use_of_mobile_phones_2014.pdf (Accessed 15 November 2015)
- Home Office, Good Practice Guidance for the Moderation of Interactive Services for Children Updated 2010, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251457/industry_guidance_moderation.pdf (Accessed 12 November 2015).
- McAfee Digital Deception Study 2013: Exploring the Online Disconnect between Parents & Pre-teens, Teens and Young Adults, Available at http://www.mcafee.com/us/resources/reports/rp-digital-deception-survey.pdf (Accessed 16 November 2015)
- Mediashift, Virtual Worlds for Children Entwined with Real World, available at http://mediashift.org/2007/06/virtual-worlds-for-kids-entwined-with-real-world162/ (Accessed 16 November 2015)
- Microsoft, How to help your children' use social networking web sites more safely, http://www.microsoft.com/security/online-privacy/social-networking.aspx (Accessed 16 November 2015)
- Mitchell, K.J., Jones, L.M., Finkelhor, D. & Wolak, J. Trends in Unwanted Exposure to Sexual Material: Findings from the Youth Internet Safety Studies. Crimes against Children Research Center, Available at http://www.unh.edu/ccrc/pdf/Unwanted%20Exposure%203%20of%204%20YISS%20Bulletins%20Feb%202014.pdf (Accessed 15 November 2015)
- Mitchell, K.J., Jones, L.M., Finkelhor, D. & Wolak, J. Trends in Unwanted Online Experiences and Sexting: Final Report. 2014. Durham, NH: Crimes against Children Research Center, Available at http://scholars.unh.edu/cgi/viewcontent.cgi?article=1048&context=ccrc (Accessed 15 November 2015)
- Ofcom Report on Internet safety measures, Strategies of parental protection for children online, 2014, Available at http://stakeholders.ofcom.org.uk/binaries/internet/internet-safety-measures.pdf (accessed 13 November 2015)
- Pacific Telecommunications Council, Broadband Policy in South Korea, http://www.ptc.org/ptc12/images/papers/upload/PTC12_Broadband%20Policy%20Wkshop_Jamie%20Ahn.pdf (Accessed 13 November 2015)
- Smith, P.K., Thompson, F., Davidson, J., Cyber safety for adolescent girls: Bullying, harassment, sexting, pornography, and solicitation, Available at http://www.researchgate.net/publication/264902151_Cyber_safety_for_adolescent_girls_Bullying_harassment_sexting_pornography_and_solicitation (Accessed 15 November 2015)
- UK Council for Child Internet Safety, Good practice guidelines for the providers of social networking and other user interactive services, updated 2010, 2010, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251456/industry_guidance_social_networking.pdf (Accessed 12 November 2015)
- UNICEF, Innocenti Research Center, Child Safety Online, Global challenges and strategies, Available at http://www.unicef.

org/pacificislands/ict_eng.pdf (Accessed 15 November 2015)

- WSIS+10 High Level Event Outcome Documents available at http://www.itu.int/net/wsis/implementation/2014/forum/inc/doc/outcome/362828V2E.pdf
- There are many excellent resources available for delivering e-safety messages. The following lists are not exhaustive, and further resources can be found at https://www.betterinternetforkids.eu/web/portal/resources
  http://www.childnet.com
- A resource for children, young people, parents and teachers on safe internet use.
  http://www.kidsmart.org.uk
- Another useful resource for children, young people, parents and teachers on online safety
  http://www.webwise.ie
- A resource for parents and teachers on safe Internet use
  http://www.digizen.org
- The site provides information for educators, parents, carers, and young people to strengthen their awareness and understanding of what digital citizenship is and encourages users of technology to be and become responsible DIGItal citiZENS.
  https://www.iwf.org.uk
- Internet Watch Foundation: Protection Online
  http://www.thinkuknow.co.uk/teachers/training.aspx
- Ambassador programmes, for training of trainers
  http://www.saferinternet.at/tipps/fuer-eltern/Educational materials.
- Austrian Awareness Center that supports children, youth, parents and educators, in safer use of digital media
  https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
- NSPCC: Children and the Internet
  http://www.internetsanscrainte.fr/le-coin-des-juniors/dessin-anime-du-mois
- Vinz et Lou – a number of French cartoons aimed at raising awareness of e-safety issues.
  http://www.teachtoday.eu/en/Lesson-Plans.aspx
- This site provides a range of lesson plans, which have been designed for use in schools.
  http://dechica.com
- An awareness raising game for small children developed by the Bulgarian Node.
  www.microsoft.com/cze/athome/bezpecnyinternet
- Czech version of the entertaining brochure on how to use the Internet safer published by Microsoft. Promoted during Safer Internet Day 2009.
  https://www.youtube.com/user/saferinternetlv/videos
- Videos on safer Internet. Langauge Latvian
  http://www.medieradet.se/ovrigt/inenglish.579.html
- A part of the Swedish Media Council's website is dedicated to moving image material Language(s): Swedish and parts in English.
  http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx
- European Research on Cultural, Contextual and Risk Issues in Children's Safe Use of the Internet and New Media.
  http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/
- Snapshot of children and internet trends in several countries
  http://www.pewinternet.org/
- Pew provides a wide range of reports into use of the Internet and related technologies. Although US based, time has shown that trends which start in the US tend to migrate to the EU in time.
  http://www.unh.edu/ccrc/
- Research from the Crimes Against Children Research Center

Appendix 1

Built-in Protection for PCs and MACs

PCs and Macs have parental controls built into their operating systems, including in each of their newest systems (Windows 10 and Mac's OS X El Capitan).

To use your computer's controls, first set up individual user accounts for each of your kids. Check your computer's user guide if you're not sure how to do this.

Mac users: Next, choose System Preferences on the Apple menu, and click on Accounts. For each child's account, click on Parental Controls and you'll be given a list of categories (Mail, Safari, etc.) that you can restrict or monitor. You can record IM conversations and designate with whom the child can talk via e-mail or iChat, among other things. You can also limit screen time. For instance, you can set the computer to automatically log your kids out at 8 p.m.

Windows users: The parental controls are accessed through the Control Panel. Look for User Accounts and Family Safety Control Panel. With Windows 10 (including with some older version of windows), you'll be given choices about web restrictions and also have the option of receiving reports on your child's use of the computer. You can designate certain hours off-limits and block objectionable video games and programmes.

No matter which system you have, most browsers (Safari, Chrome, Firefox, etc.) have an automatic history log that shows which sites have been visited. Check your user manual to learn how to check the history, if you're not familiar with it. Make sure to check all the browsers on your computer if you have more than one. And be warned: Kids can learn how to delete the history to cover their tracks, so ask questions if you discover that the history was cleared by someone other than you.

Need more help? Both Apple (Macs) and Microsoft (Windows) have online tutorials and detailed info on their websites -- just Google "parental controls" and "Apple" or "Microsoft" to find them.

Keep in mind that any protection you give your kids will, of course, be incomplete. You need to communicate with your children as much as possible and discuss with them about child online protection issues.

Protection for mobile devices

Parental controls for more safer and secure online experience for children and young people are available for mobile devices as well. Many mobile phone service providers have different fee-based options for controlling privacy and usage, filtering content and location and monitoring settings. Parental control services on mobile phones can be used to block picture messaging, block unknown phone numbers, limit what time your child can text or call, filter web browsing, and use GPS tracking to keep tabs on their physical location. Check with your mobile phone service provider on parental control packages that are available to you.

In addition many free, or low-cost parental control apps are available for smartphones that can block offensive Web content and let you monitor your child's activities on their mobile device. Parental control apps simply replace the default mobile browser with a "safe browser." These browsers block offensive links from appearing in your child's search results. Parental monitoring apps also typically let you see your child's browsing history from a remote Web portal.[1]

There are also several resources available online those explain parental control features that are inbuilt into Android phones, Iphones and tablets. For more details on how to activate those look into their online tutorials.

However, no single parental control tool is completely effective at blocking all inappropriate content — but they can reduce the likelihood of accidental discovery. As mentioned earlier, ultimately strong communication with children and young people about their online activities is the most effective tool in keeping them safe online.

1 http://www.pcmag.com/article2/0,2817,2407509,00.asp (Accessed 14 November 2015)

Appendix 2

Instant language, decoded

Abbreviations and code words speed up instant messaging and texting, but they also mask what people are saying! Brace yourself. Here are some commonly used terms:

ADIH: Another day in hell

A/S/L: Age, sex, location

BTDT: Been there done that

CULTR: See you later

GTFO: Get the f-ck out (expression of surprise)

H8: Hate

ILY or 143 or <3: I love you

JK or J/K: Just kidding

KWIM: Know what I mean?

LLS: Laughing like sh-t

LMIRL: Let's meet in real life

LYLAS (B): Love you like a sister (brother)

NIFOC: Naked in front of computer

PAW or PIR or P911: Parents are watching or Parent in room (drop the subject)

POS: Parent over shoulder (can also mean "piece of sh-t," used as insult)

Pr0n: Intentional misspelling of "porn"

STFU: Shut the f-ck up (expression of surprise rather than reprimand)

TMI: Too much information

TTFN: Ta ta, for now (goodbye)

WTF: What the f-ck?

Source: http://www.parenting.com/article/Mom/Relationships/How-to-Spy-on-Your-Child-Online/3

Photo credits: www.shutterstock.com, Violaine Martin/ITU, Ahone Ayeh Njume-Ebong/ITU

International Telecommunication Union
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int/cop

Printed in Switzerland
Geneva, 2016

ISBN: 978-92-61-16521-5

With the support of:

CHIS

THE UNIVERSITY OF EDINBURGH

ins@fe

CYBER Peace Initiative

enisa European Network and Information Security Agency