Guidelines for Children on Child Online Protection

www.itu.int/cop

ACKNOWLEDGEMENTS

Table of Contents

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 stakeholders who contributed to the text.

In an era of 'always-on' Internet, child online protection is a critical issue which, with the borderless nature of the Internet, requires a global, coordinated response.

By using computers and mobile devices to access the Internet, children and young people can do a great deal to combat and guard against cyber threats themselves, and I hope this guide will help them do so.

Mr Houlin Zhao
Secretary-General of the International Telecommunication Union (ITU)

Getting started

What are these Guidelines about?

This manual contains Guidelines for children and young people in all parts of the world on how to keep themselves and others safe online. 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, the advice or recommendations fits these different contexts.

How should these Guidelines be used?

These Guidelines have been prepared in the context of the Child Online Protection (COP)[1] Initiative in order to establish the foundations for a safe and secure cyberworld not only for today's children but also for future generations. These Guidelines are meant to act as a blueprint, which can be adapted and used in a way that is consistent with national or local customs and laws.

While older children will be able to grasp the ideas in the manual directly, younger children will need support to understand the context fully. Parents, teachers, caregivers and other adults supporting children to use these guidelines should remember that while broad guidelines can be

useful, 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.

Moreover certain subjects contained in this manual can be sensitive such as online sexual exploitation and abuse of children. Working with younger children on this issue should be approached carefully. It is important that the explanations and the messages you give to children about such issues are appropriate to their age and development. Encourage children to ask questions and state their opinions.

Why are these Guidelines important?

The information society in which today's children and young people are growing up, offers an instant digital world through the click of a mouse. An unprecedented level of services and information is accessible through a computer or a mobile device with Internet access. The barriers associated with the cost of these devices and access to the Internet are diminishing rapidly. All these technical developments provide children and young people with unparalleled opportunities to explore new frontiers and meet people from faraway places. Children and young people are truly becoming digital citizens in an online world that has no borders or frontiers.

ABCDEFGHIJKLM

1234567890123456 7

LOVELOVELOVELOVE

1 2 3

More often than not, this is a positive and educational experience: one that assists

younger generations in better understanding both the differences and commonalities of the people of the world. However, children and young people also need to be aware of some of the potentially negative aspects of the technologies.

Harmful activities can include bullying and harassment, identity theft and online abuse (such as children seeing harmful and illegal content, or being exposed to grooming for sexual purposes, or the production, distribution and collection of child abuse material).

These are all threats to children and young people's well being and a challenge that must be addressed by all stakeholders, including children themselves. Whilst all providers of online services should do whatever they can at a technical level to make the Internet as safe as it can be for children and young people, the first and best form of defence in protecting YOU is making you aware of what can happen online and make you understand that there is always a solution to a problem that you may encounter online. Empowering children and young people through education and awareness raising is therefore of paramount importance.

Moreover there is now a substantial body of international commitments, law and international instruments which underpin and in many cases mandate action to protect children both generally, and also specifically in relation to the Internet. Those commitments, laws and instruments form the basis of these Guidelines.

The United Nation's Convention of the Rights of the Child (CRC)[2] and specifically the outcomes of The World Summit on the Information Society (WSIS) (2003-2005)[3], WSIS+10 High Level Event Outcome Documents (2014)[4] and the outcomes of the United Nations General Assembly Overall Review of the Implementation of the WSIS Outcomes (2015)[5] recognize the needs of children and young people to be protected in cyberspace. The Sustainable Development Goals (SDGs)[6] 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.

Through these Guidelines, the COP Initiative calls upon all stakeholders, including children and young people, to promote the adoption of policies and strategies that will protect children in cyberspace and provide safer access to all the extraordinary opportunities and resources that are available online. It is hoped that this will not only lead to the building of a more inclusive information society, but also enable countries to meet their obligations towards protecting and realizing the rights of children as stated in the CRC, the WSIS Outcomes Document and now in the SDGs.

---

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

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

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

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

6   http://www.wvi.org/united-nations-and-global-engagement/publication/child-friendly-version-proposed-post-2015-goals

1. Background

Online technologies present many possibilities to communicate, learn new skills, be creative and contribute to establishing a better society for all, but often they also bring new risks e.g. they can expose children and young people to potential dangers like illegal content, viruses, harassment (e.g. in chat rooms), the misuse of personal data or grooming for sexual purposes. There is no silver bullet solution to protect children and young people online. This is a global issue that requires a global response from all segments of society, including children and young people themselves.

Recognising the grave dangers that may face children and young people in cyberspace, the international community has made a number of agreements and laws that protect children and young people from any kind of harm online. While these international instruments recognise that governments are foremost responsible to take action to keep children and young people safe in relation to the Internet, they also recognise the important role children and young people can play in keeping themselves and other children safe online.

The CRC, approved by the United Nations in 1989, is the most important and significant legal tool in the defence and promotion of children and young people's rights. The CRC recognises the human rights of all children in all parts of the world, including children's right to be protected from any kind of violence and harm, including in cyberspace. It also recognises children's right to

participate in keeping themselves and others safe. The CRC is also the most universally accepted convention in history. This means most governments agree to fulfill the rights that are set out in the CRC.

Further, the WSIS which was held in two phases in Geneva (from 10 to 12 December 2003) and in Tunis (from 16 to 18 November 2005) concluded with the approval of the WSIS Outcome Documents which made 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."

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 recognized "the role of ICTs in the protection of children and in enhancing the development of 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, and developed proposals on a new vision beyond 2015.

The WSIS+10 High Level Event Outcome Documents[7] 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 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.

The global community of children and young people further stated in the Outcome Document of the World Congress III against Sexual Exploitation of Children and Adolescents held in Brazil in 2008[8] the following: "We ask for strong cyber safety rules which are well propagated on both the websites and within the communities. To this end we call for the increased development of children's, teachers', parents' and family manuals which address the threats of the Internet in addition to providing supplemental information about Sexual Exploitation of Children."

The African Union has also adopted the Africa Cyber Security Convention in 2014, which highlights ways to address child pornography in the region.

The latest international agreement that secures children's rights is the commitment made by world leaders to achieve the Sustainable Development Goals (SDGs). The SDGs are a set of 17 goals and 169 targets that guide global efforts to end poverty, fight inequality and injustice and tackle climate change by 2030. These goals build upon the Millennium Development Goals (MDGs), which will expire at the end of 2015. Target 16.2 of the SDGs says that abuse, exploitation, trafficking and all forms of violence and torture against children and young people must end by 2030. This includes any kind of abuse and exploitation faced by children and young people online. The States are now further obligated to work towards making cyberspace safe for children and young people.

---

7   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

8   http://www.ecpat.net/sites/default/files/ECPATWCIIIReport_FINAL.pdf

Case Study: Children and Young People's Voices[9]

The World Congress III against Sexual Exploitation of Children and Adolescents took place in Rio de Janeiro, Brazil, from 25 to 28 November 2008. There were 3,500 participants including 300 adolescents – 150 of which were from foreign countries.

It concluded with an outcome document called the "Rio de Janeiro Declaration to Prevent and Stop Sexual Exploitation of Children and Adolescents", which contains the "Adolescent Declaration to End Sexual Exploitation". Here are some of the key messages from children and young people to the world:

We the children of the world commend the Government of Brazil and the other governments and responsible agencies for giving us the children, the present and future of the world, a voice at this World Congress III

…

7. We are at this moment calling for governmental actions to effectuate laws and policies that redound to the benefit, protection and well-being of children both on the local and international level. However, it is simply not enough to allow governments to make empty promises to curb this attack on children. Consequently, we the children, ask that action committees be created to audit the action plans in each country.

8. We also call for the adoption of an International Day where children will lead the effort in awareness raising campaigns, rallies and marches. To further enlarge the scope of this day, we request the organization of an International Art, Essay and Speech competition which will culminate on this day.

9. We now turn our attention to the media particularly the Internet which poses one of the greatest threats to millions of children throughout the world.

10. We the children must make known our plight for governments to pursue strict and punitive legislation with regards to the Internet, especially child pornography- simply another form of abuse.

11. We similarly ask for strong cyber safety rules which are well propagated on both the websites and within the communities. To this end we call for the increased development of children's, teachers, parent's and family manuals which address the threats of the internet in addition to providing supplemental information about sexual exploitation of children.

12. Further, we provide a mandate for the media to gather documents, reports, folders, CDs, videos and other materials to increase knowledge on this issue. We the children of the world pledge to vehemently and passionately pursue these policies and to call our governments to action if we do not see positive steps being taken to end this phenomenon that continues to scourge the world today.

9   Source: http://www.iyac.net/iyac_charter.pdf The full "Adolescent Declaration to End Sexual Exploitation" can be found at: http://www.unicef.org/brazil/pt/br_IIIWC_En.pdf

"Children and young people online should be aware of the opportunities"

2. Children and young people's use of technology

Information and Communication Technologies (ICTs) are changing the way children interact with their peers, the way they access information, express their views, post and share creative content. Children and young people specifically like the highly interactive nature of many Internet related services. In general, for children, the Internet is something they feel secure about, something they like, and something interesting, fun, relaxing, useful, and friendly.

Access: A study in the United States[10] finds that the age of accessing the Internet has reduced a lot. About 80% of children under the age of five years use the Internet weekly. Moreover as children get older, their use of the Internet also ncreases. In the United States about 42% and 36% of 8-11 year old boys and girls,

---

10 http://content.usatoday.com/communities/technologylive/post/2011/03/study-80-percent-of-children-under-5-use-internet-weekly/1#.VkDrLOvNz8E (Accessed 9 November 2015)
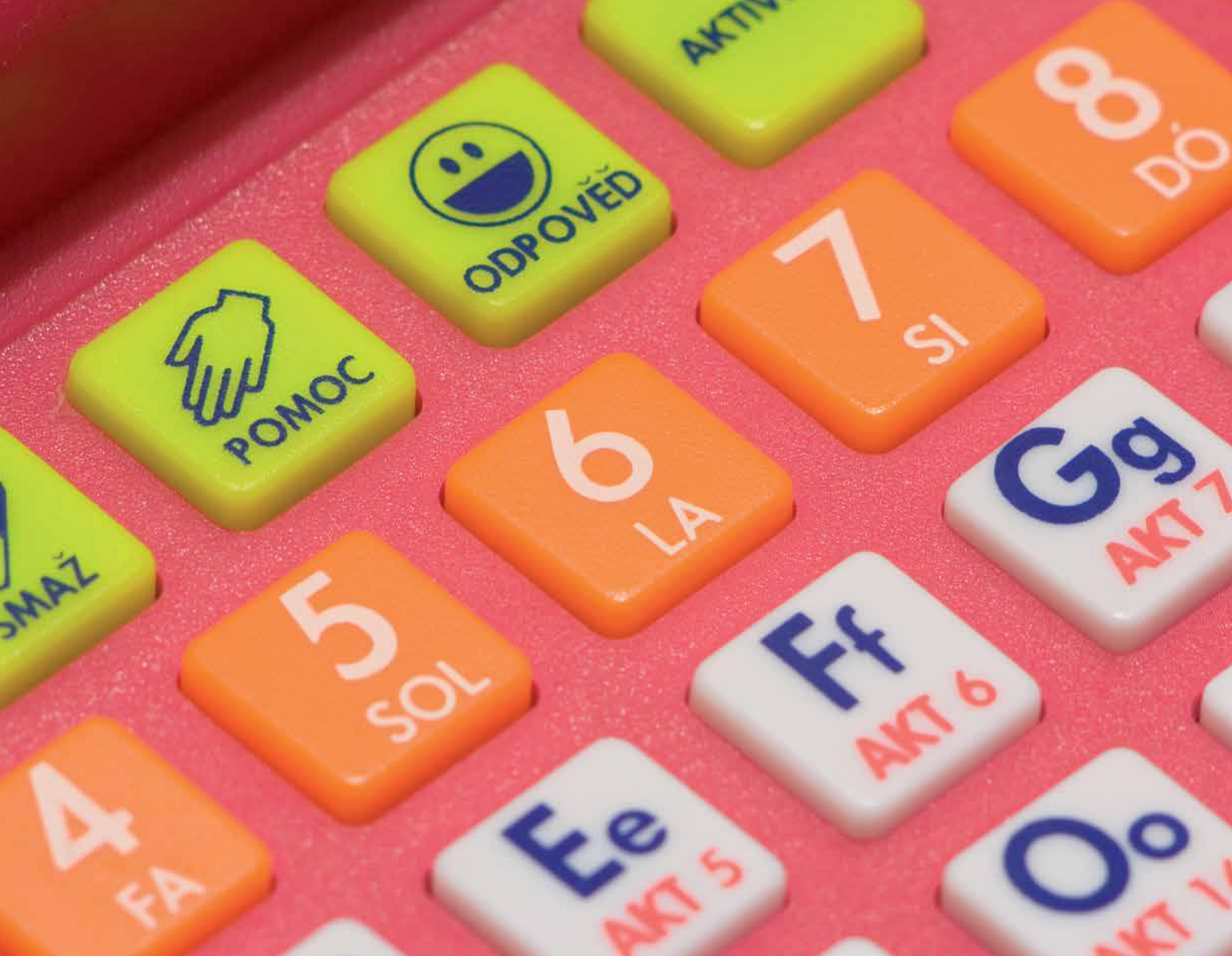
respectively, use the Internet many times a day and around one-fifth do so daily.[11] More than 90% of teens report going online daily — including about 25% who say they go online "almost constantly".[12] Across the world in South Korea, which is considered the world's most wired country, government data says about one in ten South Korean children between the ages of 10 and 19 are addicted to the Internet.[13]

Children under nine years old enjoy a variety of online activities, including watching videos, playing games, searching for information,

doing their homework and socialising within children's virtual worlds. The range of activities increases with age.[14] Listening to music, watching video clips and social networking top the list of activities done on a daily basis by 9-16 year olds as revealed in study of European children and young people. Other social activities that rate fairly high include using Skype and WhatsApp. Other activities such as searching for information to satisfy a curiosity, schoolwork, playing games (alone or in multiplayer games) are part of the daily media diets of around one in three children.[15]

The widely available fixed broad-band Internet access in the developed countries is still the preferred way of getting online, in comparison to developing countries where such infrastruc-tures are less developed. In many countries Internet cafés and other communal resources are also important providers of access for children and young people. They are likely to remain so for some time.

In recent years however mobile Internet access has increased tre-mendously. In the Asia Pacific re-gion, the fastest growing region in

relation to mobile subscriptions, China and India have become leaders in the technology with about 980 million mobile phone subscribers in India alone[16]. The world's mobile connections now number seven billion[17] – more than 230 million of which include Mobile Broadband[18]. In Latin America, mobile broadband is now more widespread in the region than fixed broadband, due to the affordability of mobile devices and the growing coverage of mobile networks.[19] Australian statistics show that in 2015 35% of children aged 8 to 11 years own a mobile phone, which is

11 http://www.emarketer.com/Article/Most-US-Children-Use-Internet-Least-Daily/1010789#sthash.bZFoyZxz.dpuf (Accessed 25 November 2015)

12 Pew Research Center, Teens, Social Media & Technology Overview 2015, Available at: http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/ (Accessed 9 November 2015)

13 http://www.businessinsider.com/south-korea-online-gaming-addiction-rehab-centers-2015-3 (Accessed 10 November 2015)

14 Holloway,D., Green, L. and Livingstone, S. Zero to eight. Young children and their Internet use. 2013. LSE, London: EU Kids Online. Available at: http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf (Accessed 2 November 2015)

15 Mascheroni, G. and Ólafsson, K. Net Children Go Mobile: risks and opportunities. Second Edition 2014. Milano: Educatt. Available at: http://eprints.lse.ac.uk/56986/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Net%20Children%20Go%20Mobile%20Project_Reports_Net%20children%20go%20mobile%20risks%20and%20opportunities%20%282nd%20ed.%29.pdf (Accessed 3 November 2015)

16 Press Release, Telecom Regulatory Authority of India, 2015, Available at: http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/PR-No=47.pdf (Accessed 2 November 2015)

17 http://www.itu.int/net/pressoffice/press_releases/2015/17.aspx#.VjgW7OvNz8E (Accessed 2 November 2015)

18 https://mobiforge.com/research-analysis/global-mobile-statistics-2014-part-a-mobile-subscribers-handset-market-share-mobile-operators (Accessed 2 November 2015)

19 Economic Commission for Latin America and the Caribbean (ECLAC), The new digital revolution: from the consumer Internet to the industrial Internet, 2015. Available at http://repositorio.cepal.org/bitstream/handle/11362/38767/S1500587_en.pdf?sequence=1 (Accessed 26 November 2015)

twice as many as in 2007.[20] It is clear children and young people are now increasingly using mobile devices to go online, including smartphones and tablets.

Digital devices: There are number of digital devices through which children and young people now go online such as desktop computers, laptop computers, mobile phones, smartphones, tablets, other handheld devices such as iPod Touch, e-book readers and games consoles.

A 2014 study in the UK shows that more than a third of 12-15 year olds access the Internet through a smartphone. Moreover the tablet is the one media device that has grown most in popularity amongst 5-7 year olds over the last year, with 54% using it in 2014 as compared to 39% in 2013. At the same time, access to a PC or laptop in the home for children aged 5-15 years has been declining.[21] This has also resulted in high use of social media applications (such as Facebook, Twitter, Whatsapp) especially through mobile apps. Similarly in Brazil, in 2013 a little over half of the children (53%) use the mobile phone to access the Internet. In 2012, this population was 21%. Internet access through tablets went from 2%, in 2012, to 16% in 2013.[22]

However children and young people experience slightly increased risk of harm when accessing the Internet via a smartphone or tablet, as they are less likely to be monitored by parents or caregivers. Children with smartphones also access the Internet more often, engage in a greater range of activities, and have a higher number of online skills.[23]

The increased used of Internet through smartphones also provide several benefits. For example, a range of educational services could be provided via mobiles to children in remote villages and communities. Mobile phones could serve as an essential means for children to become connected to one another for educational and peer-learning activities. These are particularly important for communities that are either nomadic or have been displaced due to natural disasters, war civil strife or other major disruptive events.

Information: The access to information is crucial for children and adolescents when doing their homework. A study on children's Internet usage in the UK[24] indicates that 75% of children aged 8-11 years and 84% of adolescents aged 12-15 years use the Internet to help them with their homework. Similarly in Brazil, 87% of children and young people aged 9-17 years use the Internet for schoolwork.[25] The library has moved online and the ability to seek and find relevant and reliable information in any language is a great advantage which has been embraced by the young generation throughout the world.

20 https://kids.ownfone.com.au/children-and-cell-phones-statistics#.VldJvITtkhY (Accessed 26 November 2015)

21 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 26 November 2015)

22 ICT Kids Online Brazil 2014, Available at http://cetic.br/media/docs/publicacoes/2/tic-kids-online-2013.pdf (accessed 10 November 2015)

23 Stald, G., Green, L., Barbovski, M., Haddon, L., Mascheroni, G., Ságvári, B., Scifo, B. and Tsaliki, L. Online on the mobile: Internet use on smartphones and associated risks among youth in Europe. EU Kids Online 2014. Available at: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/MobileReport.pdf (accessed 13 November 2015)

24 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 25 November 2015)

25 ICT Kids Online Brazil 2014, Available at http://cetic.br/media/docs/publicacoes/2/tic-kids-online-2013.pdf (Accessed 25 November 2015)

One of the most used resources online is Wikipedia[26]. Wikipedia is a multilingual, Web-based, free-content encyclopedia project, where you can read, edit and write articles on any subject or issue you find relevant. Fact finding exercises can easily lead you from one page on to the next and so on. The search for new information is never boring and with the increased localisation of content, the language barriers slowly diminish.

Social networks: The birth of online social networks has been a remarkable success. The variety of social networks caters to all ages, cultures and languages. Having a profile on a social network has become an important part of many children and young people's online lives. When home from school, the ability to continue your discussions with your friends online whilst doing your homework, sending SMS's and listening to music (frequently at the same time!) is a picture many will recognize. Social networks can often represent a one-stop gateway to games, friends, news, music, and ways of self-expression. In other words, you can be creative, funny, reflective and entertained by using ICT's.

Social networking tends to top the activities taken up by children on a daily basis, and children who also use a smartphone and a tablet to go online are more likely to engage in activities on a social networking site every day. Overall, about 70% of children and young people have at least one profile on a social networking site in Europe[27]. On the same lines, about 80% of Internet users between the ages of 9 and 17 years have social networking profiles in Brazil, reveals the ICT Kids Online Brazil 2013 survey.[28] Among these studies, Facebook emerges as the most commonly used social networking site among children and young people.

In the UK one in four children use Twitter the most to socially network in the online world. Sharing photos, videos and other content are other most popular online activities. Most children and young people in Europe also have a profile on a media-sharing platform such as YouTube, Instagram or Flickr.[29]

An example of young people creatively using media sharing platforms could be that of a young band that creates a new song, posts the video on YouTube[30], and informs their friends and fans about it. The fans can then see this song by streaming it online on their mobile phone, tablet or PC. If they like the song, they will spread the word by telling their friends, who will then tell their friends and so on. With simple techniques and little financial investment, this band can now gain a greater fan base and potentially be heard by

26 http://en.wikipedia.org/wiki/Main_Page

27 Mascheroni, G. and Ólafsson, K. Net Children Go Mobile: risks and opportunities. Second Edition 2014. Milano: Educatt. Available at: http://eprints.lse.ac.uk/56986/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_ shared_repository_Content_Net%20Children%20Go%20Mobile%20Project_Reports_Net%20children%20go%20mobile%20risks%20and%20opportunities%20%282nd%20ed.%29.pdf (Accessed 3 November 2015)

28 ICT Kids Online Brazil 2014, Available at http://cetic.br/media/docs/publicacoes/2/tic-kids-online-2013.pdf (Accessed 10 November 2015)

29 Mascheroni, G. and Ólafsson, K. Net Children Go Mobile: risks and opportunities. Second Edition 2014. Milano: Educatt. Available at: http://eprints.lse.ac.uk/56986/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_ shared_repository_Content_Net%20Children%20Go%20Mobile%20Project_Reports_Net%20children%20go%20mobile%20risks%20and%20opportunities%20%282nd%20ed.%29.pdf (Accessed 3 November 2015)

30 https://www.youtube.com

a record company that wishes to sign them to their label. Stories now abound of bands promoting their songs via services like YouTube and ending up with a record deal.

This is not so different from the offline world, but the ability to reach a larger audience in a shorter time is one of the great advantages of ICT's. In essence, a service might take off slowly but reach critical global mass in a very short time due to the ability of the children and young people to instantly share their experiences with friends.

Virtual worlds for children and teenagers: In these worlds, children can often create an avatar and, with it, explore an imaginary universe. They can play games, chat and decorate virtual rooms or other spaces. In 2012, there were over 150 virtual worlds either operating or in development which are aimed at children and young people under 18 years of age[31], according to K Zero, a consulting firm. These sites have around 355 million registered users under the age of 10 and over 800 million aged 10 to 15 years.[32]

Webkinz, Neopets and Club Penguin are some of the virtual worlds that are particularly popular with children aged eight and under, while children over ten years tend to prefer the virtual worlds of Poptropica, Moshi Monsters and Moviestar Planet.[33]

31 http://www.kzero.co.uk/blog/young-children's-play-in-online-virtual-worlds/ (Accessed 3 November 2015)

32 Burke. A., Children's Construction of Identity in Virtual Play Worlds – A Classroom Perspective, 2013, Memorial University, Available at: http://ejournals.library.ualberta.ca/index.php/langandlit/article/viewFile/19779/15290 (Accessed 3 November 2015)

33 http://www.kzero.co.uk/blog/category/universe-graph/ (Accessed 3 November 2015)

Virtual worlds such as Wizard 101, Roblox and Minecraft are popular with children aged 12-14 years. However among 14 – 15 year olds, girls become more engaged than boys, showing the popularity of fashion based virtual worlds such as Stardoll and GoSupermodel. The Stardoll has about 250 million global accounts. As evident there are virtual worlds catering to each specific age group and gender.[34]

Virtual worlds, like Club Penguin, that target primary and elementary school children, allow users to create a profile and take on the identities of penguin avatars[35] to play game and activities. All users will have to design their own avatar with easy to use tools. The ability to appear as an avatar allows for everyone,

regardless of their real world physical appearance, to enter a community where all are equal and prejudice does not exist.

Taking on this new identity can allow for the user to express themselves differently, testing a new profile or attitude, being bold and upfront on issues that matter to them, or even just live 'some- body' else's life for a while. Needless to say that there are rules that need to be followed, but the ability to test a different personality can be a fun experience.

What's your online profile?: An interesting study with Habbo Hotel's (a virtual world targeting 13 years and older)[36] users reveals the digital profiles of teens online:

Achievers	Ambitious, strong minded and materialistic. They value material success and whilst having lots of friends do not consider other people's feelings as much as other segments
Rebels	Value gathering lots of experiences in life and enjoy a fast-paced lifestyle. Like Achievers they want to become "rich and famous", but they are not willing to compromise on having fun in order to achieve this goal
Traditionals	Value having an ordinary life and see themselves as honest, polite and obedient. They are keen to help others but are less ambitious and pleasure seeking compared to other segments
Creatives	Share many of the same positive traits as Traditionals, but with a focus on creativity. They place value in getting a good education and being influential in life, but they are also active, social and have an interest in travelling
Loners	More introverted and less likely than other segments to identify with any specific personality traits. They rarely see themselves as active or self-assured, but are more open minded in their attitudes compared to Traditionals or Achievers

34 http://www.kzero.co.uk/blog/category/kidstween-worlds/ (Accessed 3 November 2015)

35 Avatars in video games are essentially the player's physical representation in the game world, http://en.wikipedia.org/wiki/Avatar_(computing)

36 Habbo's Second Global Youth Survey 2008

Children and young people have online profiles and communicate with each other by posting comments or greetings on their friend's profile pages. Having many friends linked to ones profile does appear to give a high status amongst their peers, although it is questionable whether having a high number of online friends in itself is an objective to strive for. Still, 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[37].

Many social networks facilitate the creation of sub groups based on themes such as democracy, pets, games, school work music and so forth. These communities might not be available to you in your town, region, country, but here again; ICT's folds the world and brings it to your screen and offers you the possibility of experimenting with forms of participation and freedom of expression that are rarely guaranteed in their real, everyday lives in the adult world. The positive culture that reigns in online communities helps everyone to have a good experience and increases the willingness to engage with other people online and learn about new things.

Case Study: The Bright Side of Social Networks for Children with Learning Difficulties

The positive benefits from social networks for children with learning difficulties can be summarised as follows[38]:

Practicing social skills: you get a chance to meet all kinds of people online. Because socializing via technology isn't as immediate as face-to-face interactions or telephone conversations, you have a little more time to think about a situation before you respond. This is an opportunity for you to experiment with greetings, responses, etc.

Defined/guided social interaction: While online communication technologies increasingly allow for freeform interaction, social interaction can be narrowed (for purposes of scope and safety). Some examples of focused interaction online include buddy/friend lists, moderated themed chat rooms or message boards and, for younger children, the opportunity for parents to help a child by typing or reading along some of the time. This can help children build skills and confidence that will increase their independence as they mature.

Identity experimentation: A child can create an online identity that is different from what he or she normally presents. For example, a kid who really likes comics can be the "king of all superhero knowledge" online without being teased about it at school. Such a child can also find a peer group online that appreciates this aspect of him or her."

Frequent use of existing and emerging/changing technologies: Technology is evolving faster than ever before. As you learn to adapt to new technologies (or new applications of existing technologies), you will be better equipped to adapt to future technology. This will help you quickly assess the risks of communicating through these new and adapt your behaviour to maintain control over your own safety.

37 Pew Research Center, Teens, Social Media, and Privacy, 2013. Available at http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/(Accessed 9 November 2015)

38 http://www.greatschools.net/cgi-bin/showarticle/3120 (Accessed 26 November 2015)

"Be smart, responsible and safe online – just like in the real world"

Games: Classic board games have also moved online and are now played alongside what is called "massively-multiplayer online role-playing games" (MMORPGs), such as the World of Warcraft. As with social networks, online games can connect you with other players from around the world. More than 70% of gamers play with a friend and millions of people worldwide participate in massive virtual worlds.[39] A recent research in UK shows majority of children in each age group who play games online play on their own/against the computer or games player, accounting for over four in five 5-7 year olds, close to seven in ten 8-11 year olds and seven in ten 12-15 year olds[40]. The research also shows

an increase in the numbers of younger children playing games online. A 2014 Cox Internet Safety Survey reveals nearly three in four online gamers interact with other gamers online through web chat, voice chat and web cam.[41] It is indeed a social activity that captures youth universally and can be played now on the smallest of handheld devices[42].

The term "online gamer" may conjure up images of a lone teenager playing "Ever- Quest" in his parents' basement, but that's not how it is in South Korea. Group interaction is as strong a cultural tradition in that country as studying and shopping. Young people go to the PC bangs to blow off steam and to hang out. Community within games is really popular, as well as the ability to form groups, or guilds. These social aspects are a big reason why people keep playing games in South Korea."[43] However given the excessive hours spent by children and young people playing online games, South Korea passed the Shutdown law (also known as the Game Addiction Law) in 2011. The Law forbids children under the age of 16 in South Korea to play online video games from midnight to 6:00 A.M. Given the debate over this law, the Culture and Gender Equality Ministry announced in September 2014 that children aged 16 and below may be able to play online games in midnight with the approval of their guardians.[44]

The risks in online gaming also arise largely due to the minimal restrictions involved and the fact that they are not face-to-face. Because of this, children and young people cannot be sure who they are playing against and chatting to or what their motives are. Children could also be playing online games with an inappropriate age rating. A survey by Get Safe Online[45] reveals about 25% of children and young people have disclosed personal information while online gaming. About 35% of children and young people have spoken to someone they don't know while online gaming, while more than 15% of the children have been bullied or verbally abused while online gaming.

39 http://www.apa.org/news/press/releases/2013/11/video-games.aspx (Accessed 10 November 2015)

40 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 25 November 2015)

41 Cox 2014 Teen Internet Safety Survey, Available at http://www.cox.com/wcm/en/aboutus/datasheet/takecharge/tween-internet-safety-survey.pdf (Accessed on 26 November 2015)

42 The Integration Centre. Online Gaming and Youth Cultural Perceptions. Available at http://www.integrationcentre.ie/getattachment/3728d764-143f-4ece-bf9a-a0134ceda102/Online-Gaming-and-Youth-Cultural-Perceptions.aspx (Accessed 3 November 2015)

43 Adapted http://www.msnbc.msn.com/id/17175353/ (accessed 10 November 2015)

44 http://treeofsaviorgame.com/general/313/understand-game-addiction-law-in-south-korea-in-5-minutes/ (accessed 10 November 2015)

45 https://www.getsafeonline.org/safeguarding-children/gaming/ (Accessed 10 November 2015)

Digital Citizenship:

The introduction of new technologies always carries the need to understand how to use it appropriately. We, including children and young people, can demand that the producers and providers build in as many safety features as possible, enabling us to make informed choices on matters, like for instance, revealing private information. A 2015 global survey on privacy on the Internet reveals that two out of three websites and apps collect and process personal data of children, and half of the sites and apps share personal information about children with other organizations. In more than 70% per cent of these sites and apps, it was not easy to delete personal information from an account.[46]

Given this scenario, it is up to children and young people to carry the main responsibility of acting appropriately and respectfully online. Increasingly the term of digital citizenship is being used. Digital citizenship isn't just about recognising and dealing with online hazards. It's about building safe spaces and communities, understanding how to manage personal information, and about being Internet savvy - using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do the same[47].

Safer Internet celebrations:

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 who all collaborate in creating greater awareness of the opportunities to get a positive online experience. To get the most updated information on these events it is suggested you do a search online for terms like "internet safety celebration" + "country name".

---

46   https://www.getsafeonline.org/safeguarding-children/gaming/ (Accessed 10 November 2015)

47   http://www.insidemarketing.it/privacy-e-minori-il-50-di-siti-web-e-app-condivide-i-dati-di-bambini-con-terze-parti_8103/ (Accessed 25 November 2015) http://www.digizen.org/

Here is a list of issues you should consider when discussing "Digital Citizenship."[48]

Digital Etiquette: electronic standards of conduct or procedure.

- It is not enough to create rules and policy, we must learn to become responsible digital citizens in this new society.

Digital Communication: electronic exchange of information.

- Anyone should be afforded the opportunity to access information anywhere and anytime.

Digital Literacy: process of teaching and learning about technology and the use of technology.

- As new technologies emerge, we need to learn how to use that technology quickly and appropriately. We need to be digital literate.

Digital Access: full electronic participation in society.

- Digital exclusion of any kind does not enhance the growth of human beings in an electronic society. One gender should not have preferential treatment over another. Electronic access should not be determined by race, physical or mental challenges. The issue of people in cities or towns with limited connectivity needs to be addressed as well. To become productive citizens, we need to be committed to equal digital access.

Digital Commerce: electronic buying and selling of goods.

- Children and young people need to learn about how to be effective consumers in a safe digital economy.

Digital Law: electronic responsibility for actions and deeds.

- Digital law deals with the ethics of technology. There are certain rules of society that fall under illegal acts. These laws apply to anyone who works or plays online.

Digital Rights and Responsibilities: those freedoms extended to everyone in a digital world.

- Basic digital rights must be addressed, discussed, and understood in the digital world. With these rights also come responsibilities. Users, including children and young people, must help define how the technology is to be used in an appropriate manner. In a digital society these two areas must work together for everyone to be productive.

Digital Security (self-protection): electronic precautions to guarantee safety.

- In any society, there are individuals who steal, deface property, or disrupt other-people's lives. The same is true for the digital com- munity. It is not enough to trust your peers in the community for your own safety. In our own homes, we put locks on our doors and fire alarms in our homes to provide some level of protection. The same must be true in the digital world to provide protection and digital security. We need to have virus protection, backups of data, and surge control of our equipment. As responsible citizens, we must protect our information from outside forces that might cause disruption or harm.

---

48 http://www.digitalcitizenship.net/Nine_Elements.html (Accessed 26 November 2015)

"All children and young people around the world have the right to a safe experience online"

3. What you need to know to stay safe online

INTERNET SAFETY GUIDELINES:

Internet safety messages need to be timely, age specific, culturally sensitive and match the values and laws of the society in which the child or young person lives.

The COP Initiative has identified three principal age groupings of young Internet users. These groupings broadly correspond with the key stages of development on a child's journey to adulthood. Hence the guidelines can be seen as a ladder which takes you through progressive phases. However, we cannot emphasise too strongly that every child is different who requires and deserves individual attention. One size does not fit all. Nothing should ever be assumed or taken for granted.

The first age group 5-7 year old:

This group experience their first contacts with technology. Their usage should be closely supervised at all times by a parent or adult. Filtering software or other technical measures may also have a particularly useful role to play in supporting the use of the Internet by a child of this age. It would be wise to consider limiting such a young child's potential access e.g. by constructing a list of safe websites, which are age

appropriate such as a walled garden. The aim is to provide this age group with the basics in Internet safety, etiquette and understanding. This age group will probably not be able to decode more sophisticated messages. Parents or adults with responsibility for children should consult the COP guidelines for parents, guardians and educators to see how they might best assist the youngest age group to stay safe online.

The second age group: 8-12 year old:

This age span is a challenging transition for the child. Typically he or she is becoming a young person with a greater capacity to form questions. Their curiosity will start to push them to seek out and challenge boundaries, looking for their own answers. It is an age group where awareness of what is available online exists. The impulse to seek and find out what's there is great. Throughout

childhood a child is expected to test the barriers and evolve through this kind of learning. Filtering software or other technical measures may have a particularly useful role to play in supporting the use of the Internet by a young person of this age.

An important aspect of this age group is the sometimes uncritical approach to content and contact, which can put the age group in a particularly vulnerable situation for predators and commercial entities wishing to engage with them.

The last age group: 13 year old and above:

This group is the one covering the longest span, is the group consisting of young people who are, namely, teenagers. This group is growing up rapidly, transitioning from being young people to becoming young adults. They are both developing and exploring their own identities,

their own tastes. They will very often be able to use technology with a high level of proficiency, without any adult supervision or interaction. Filtering software will start to become less useful and less relevant but it certainly could continue to play an important supporting role, particularly for some young people who may have temporary or longer-term vulnerabilities.

Linked to their own hormonal development and a growing sense of physical maturity, teenagers can go through phases when they feel a very strong need to find their own way, to escape close parental or adult supervision and seek out their peers. A natural curiosity about sexual matters can lead some people in this age group into potentially worrying situations and this makes it all the more important for them to un-derstand how to stay safe online.

The COP guidelines recognize the difficulty in creating messages that will cover the needs of all ages within the defined groups. Local laws and customs are also profoundly important in matters of this kind. There is not a one-size-fits-all. The COP Initiative would be very happy to assist with adapting and localizing the content of this and any other COP Guidelines. If you wish to pursue this, you are invited to make contact via cop@itu.int.
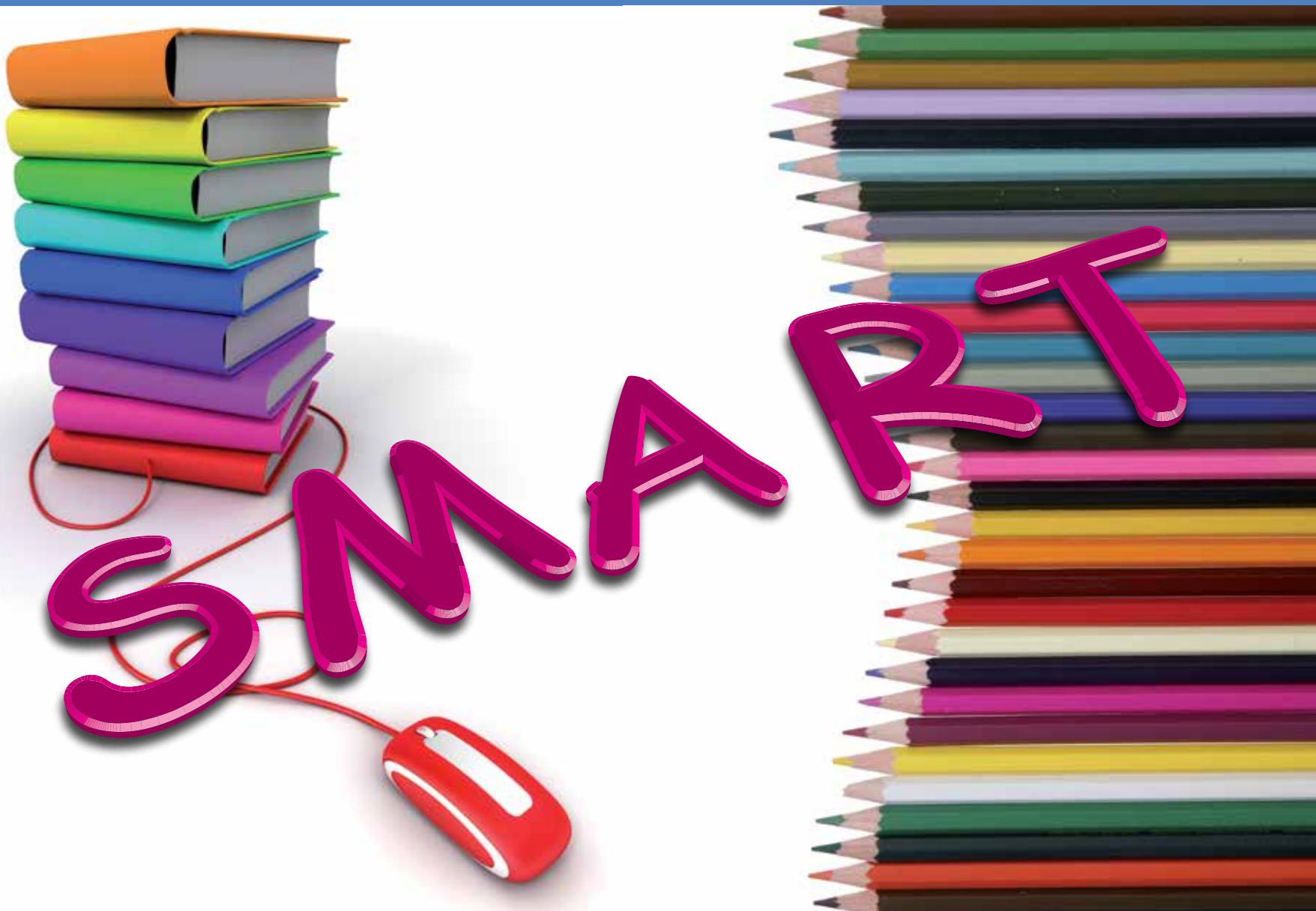
SMART

"SMART rules"
for children and young people

S = Set your limits
M = Meeting online friends offline
A = Accepting invitations/friendships
R = React
T = Tell someone about your concerns

Using the Internet is fun. Enjoy it most by keeping yourself safe

1. You can do a lot of great things on the Internet. You can play games, you can chat with your friends, meet new friends and find a lot of useful information. You have the right to enjoy and explore all that the digital world has to offer!

2. But you also have to be aware that you can find some unpleasant things on the Internet, such as images and stories that may confuse or even frighten you. Your friends and trusted adults are not the only people within this digital world. Unfortunately the Internet is also used by people who are not so nice or who might even want to harm, harass or bully you or other people. While using the Internet you need to be aware of certain basic rules to be able to safeguard yourself and others.

3. You have the right to use the Internet safely and to set your own limits. Be smart, responsible and safe online, as well as in real life!

S = SET YOUR LIMITS

1. Take care of your privacy. Whether using a social networking site or any other online service take care of your privacy and that of your family and friends. You might have the feeling of being anonymous online but collecting information from various sources can reveal too much private information about yourself for others you are close to, including your family.

2. If you join a social networking site use the privacy settings to protect your online profile so that only your friends can see it. Wherever possible instead of your real name you should use a nickname that your real friends will be able to recognize. Other interactive services, for example instant messaging, will often also provide privacy tools. Use them

3. Think twice before you publish or share anything online. Are you prepared to share it with everyone online; your close friends, as well as strangers? Once you post information, photographs or any other material on the Internet, you may never be able to remove it or prevent other people from using it. You can never know for sure where it might end up.

4. Be critical what appears to be a fact may really not be true at all. Unfortunately, if it appears too good to be true, it probably is. Always double check the information from other reliable sources.

5. You have rights and you, as well as other people, should respect them. You should never accept harassment or bullying by other people. The laws and expectations of decent and acceptable behaviour are valid online as well as in real life.
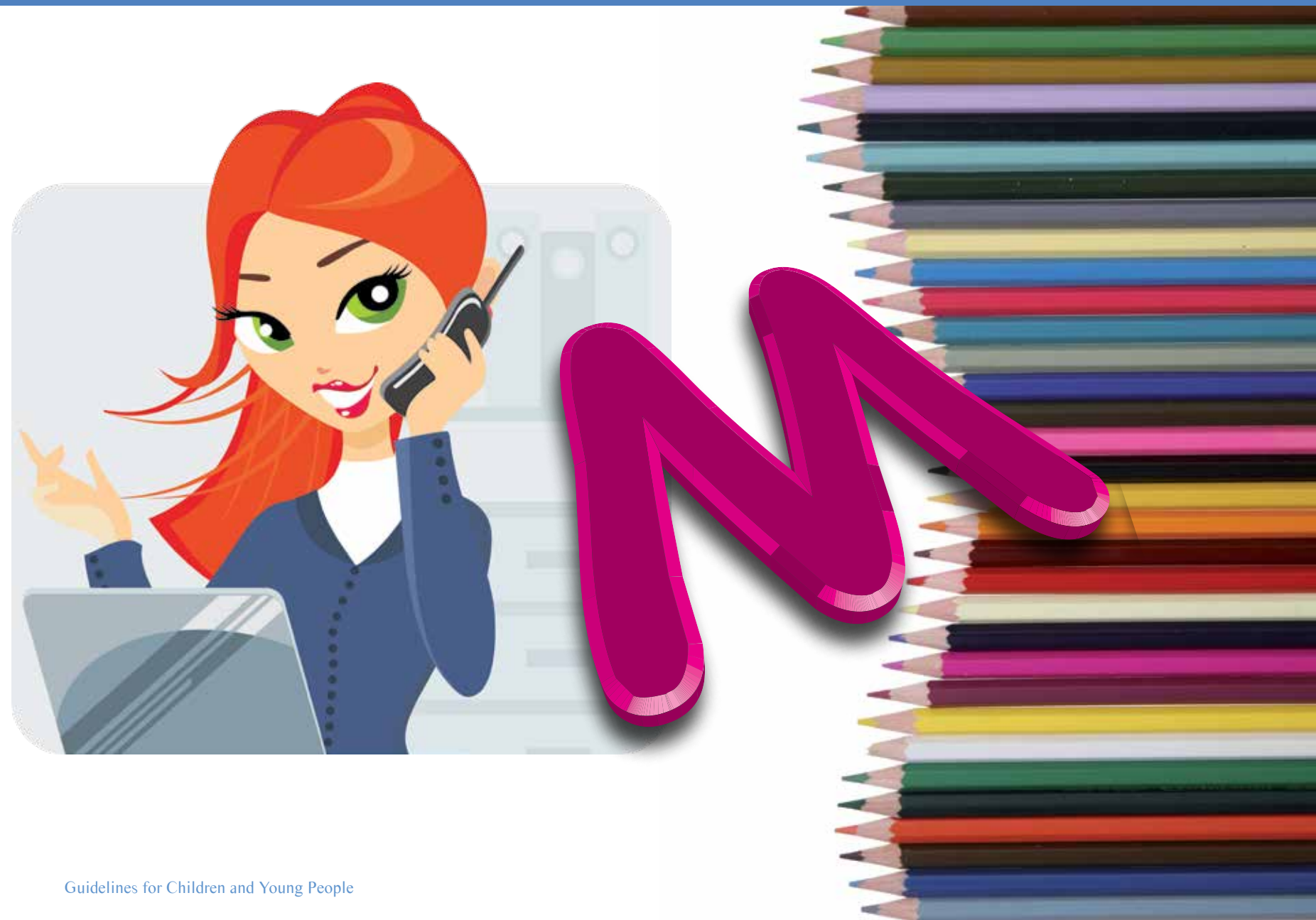
M = MEETING ONLINE FRIENDS OFFLINE

1. Sometimes online contacts develop into friendships.

2. Think twice before meeting an online friend in real life. If you still would like to meet an online friend offline, you should always take someone reliable with you. You should ask your parent or another trusted adult to join you to avoid any trouble in case the meeting turns out to be a disappointment.

3. Bear in mind that your online friend might turn out to be a different kind of person than you thought he or she would be.

A = ACCEPTING INVITATIONS / FRIENDSHIPS

1. Most of the people you communicate with online are probably already your friends in real life. You can also be connected to the friends of your friends. Very often that can be fun but at the same time if you do not actually know someone yourself, are you really prepared to count them as a "friend" and share with them exactly the same information that you share with your oldest and best friends?

2. Through online connections you can connect with people previously unknown to you. You may get requests by strangers who want to be included in your contact list and see your profile, but it is not wise to accept them. There's nothing wrong with declining invitations you are not sure about. Getting more and more contacts is after all not the point of social networking.

R = REACT

1. Protect yourself from upsetting or distressing content. Do not knowingly access or share links to such sites. If you see something that bothers you, talk about this with your parents or someone you trust.

2. Ignore bad behaviour and leave unpleasant conversations or sites with inappropriate content. As in real life there are people who for some reason, may behave aggressively, insultingly or provocatively towards others, or who want to share harmful content. Usually it is better just to ignore them and then block them.

3. Block anyone approaching you using rude, intruding or threatening emails or comments. Even if the message may be upsetting and makes you feel uncomfortable you should save it so you can show it to an adult for advice if needed. You are not the one to be ashamed of the content of the messages.

4. Always be alert if someone, especially a stranger, wants to talk to you about sex. Remember that you can never be sure of the true identity or the intentions of that person. Approaching a child or a young person in a sexual way is always a serious cause for concern and you should tell a trusted adult, so you or the trusted adult can report it.

5. If you have been lured or tricked by someone into engaging in sexual activities or transmitting sexual images of yourself, you should always tell a trusted adult in order to receive advice and help. No adult has a right to request things of that particular nature from a child or a young person - the responsibility always lies with the adult!
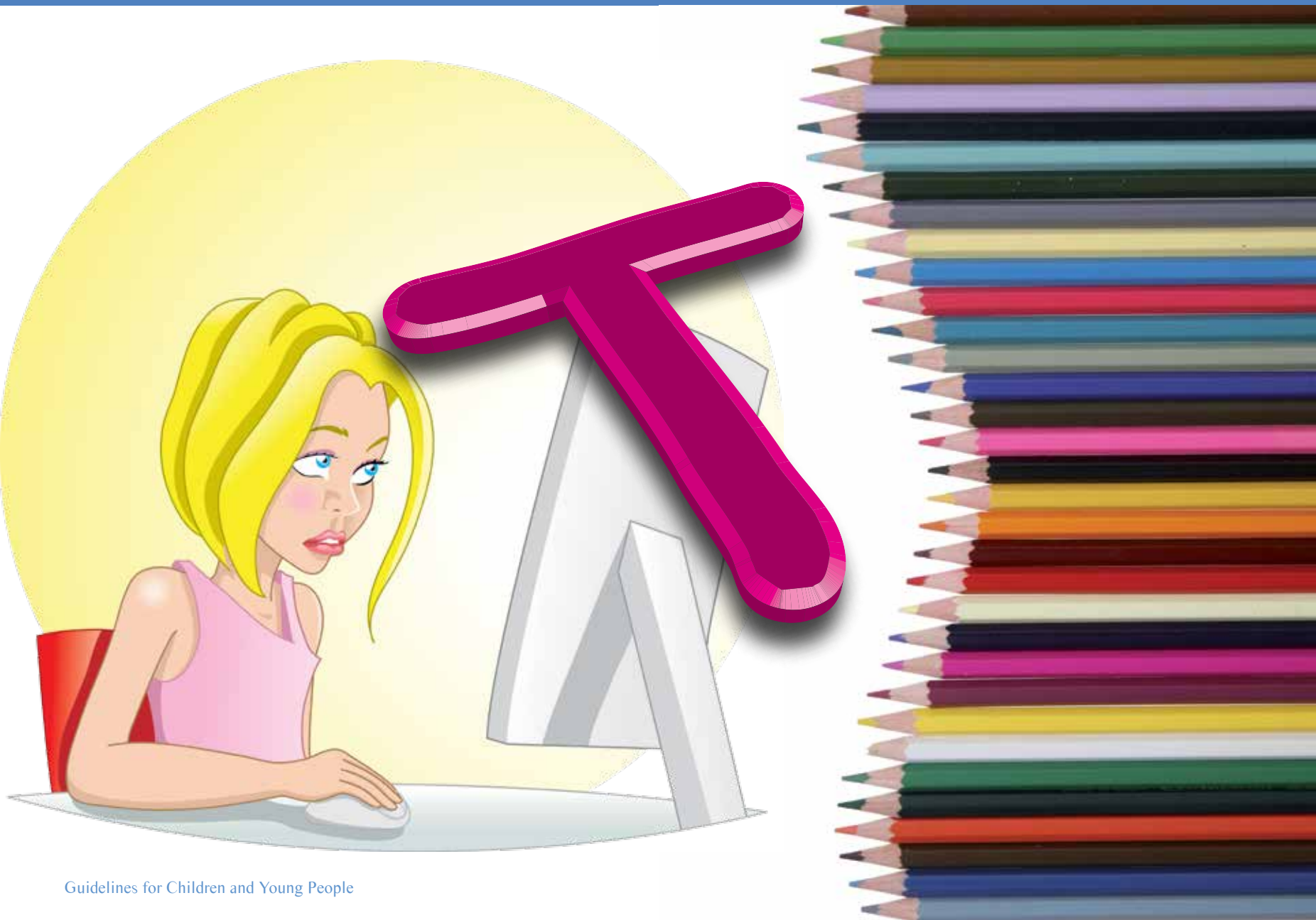
T = TELL SOMEONE ABOUT YOUR CONCERNS

1. If you have any concerns or problems while online, you need to tell someone you can trust. Your parents or some other adult can help and give you good advice on what to do. There are no problems that are too big to be solved! You might also want to call a child helpline available in your country.

2. You can report harmful or inappropriate content or activities on the websites to the abuse e-mail of the host of the site.

3. You can report illegal content to an Internet Hotline or to the police.

4. You can report illegal or possibly illegal activities to the local police.

5. In addition to taking good care of yourself, you should also take care of your computer or mobile device. Like the SMART rules, there are some easy tips to remember in order to keep your computer and mobile device safe.

49 E.g. CHI available at: www.childhelplineinternational.org
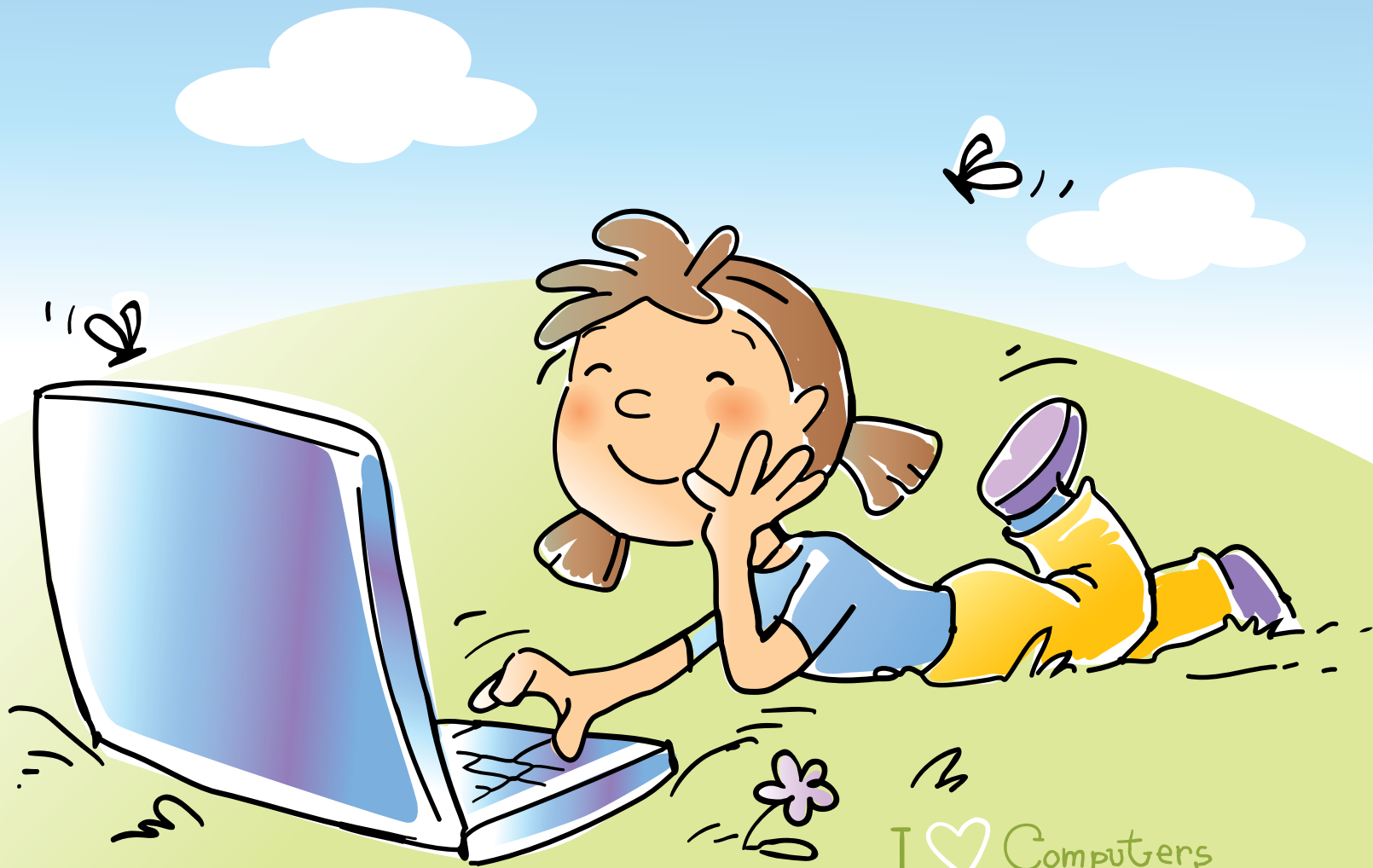
I ♥ Computers

Learn to use your machine safely:

1. Make sure you have installed and learned how to use a firewall and anti-virus software. Remember to keep them up to date!

2. Learn about your computer's operating system (like Windows, Linux, etc.) and especially about how to patch it and keep it up to date.

3. If parental controls are installed then talk with your parents and agree on the level that matches your age and needs. Don't try to crack them.

4. If you receive a file you are unsure of or don't know who has sent it, do NOT open it. This is the way Trojans and viruses infect your machine.

5. Get a feeling for your machine and how it works so that you can act if you spot something unusual.

6. Learn to check who you are connected to – learn to use tools like "Netstat" Finally, a great way to make sure that your parents agree with your online life is to set up a written agreement with them. The purpose is to reassure them that you are aware of the risks associated with being online, knowing how to behave and what to do, as well involving your parents making them understand what you actually do when you are online. The agreement needs to be based on a mutual agreement between you and your parents. There is an example of such a contract at the end of these guidelines (Appendix 1). You will be able to find different versions of a Family Internet Safety Contract online.

Your online rights

- You have the right to make use of technologies to develop your personality and help increase your capabilities;

- You have the right to protect your identity;

- You have the right to participate, have fun and access information appropriate to your age and personality;

- You have the right to express yourself freely, and be treated with respect while always respecting others;

- You have the right to be critical and discuss anything you read or come across when online;

- You have the right to say NO if someone makes you feel uncomfortable with his/her requests when online.

Guidelines for the age group 5-7 year old

Many young people in this age group will not be able to read or understand Guidelines of this kind. Their usage should be closely supervised at all times by a parent or adult as well. Filtering software or other technical measures may also have a particularly useful role to play in supporting the use of the Internet by a child of this age. It would be wise to consider limiting such a young child's potential access to the Internet e.g. by constructing a list of safe websites which are age appropriate. The aim is to provide this age group with the basics in Internet safety, etiquette and understanding. This age group will probably not be able to decode more sophisticated messages. Parent or adults with responsibility for children should consult the COP guidelines for parents, guardians and educators to see how they might best assist the youngest age group to stay safe online. In addition, several useful and interesting links to online resources for this age group have been listed in the section 'Sources for Further Reading and Inspiration'.

Guidelines for the age group 8-12 year old

There are lots of different things you can do online. While most of the time it's all great fun, sometimes things don't go as well as you hoped and you may not immediately know why or what to do about it. This section has some really helpful tips to help you be safe online.

Chatting to friends using IM, in chat rooms and on social networking sites can be great ways to keep up to date. Meeting new friends online is also fun. You can meet people online who like the same movies or sports as you. But while there are lots of good points about keeping in touch with online friends, there are also some risks with meeting people online—especially if you don't know them in real life.

To help stay safe while you chat, remember some simple tips:

1. Be careful who you trust online. A person can pretend to be someone they are not.

2. Choose your friends. While it's good to have a lot of friends, having too many, makes it harder to keep an eye on who sees the stuff you post online. Don't accept friend requests if you really don't know the person and you're not sure about them.

3. Keep your personal details private. Use a nickname instead of your real name if you are in a site or game where there may be lots of people you don't know. Ask your parents before giving anyone on the Internet your name, address, phone number or any other personal details.

4. Set your profile to private. Ask your parents to help you do this if you're not sure. It's really important.

5. Always keep your password secret. Don't even share it with your friends.

6. If you want to arrange to meet someone you've met online, check with a parent first and ask them to go with you. Always meet in a brightly lit public place where lots of other people will be around, preferably during the day.

7. If someone writes something rude, scary or something you don't like, tell your parents or another adult you trust.

Netiquette

By netiquette we mean how you should or should not behave with other people online. Sometimes it's easy to forget that the other person you are chatting to on IM, playing a game with, or posting to their profile is a real person. It's easier to say and do things online that you might not do in 'real life'. This may hurt that person's feelings or make them feel unsafe or embarrassed. It's important to be kind and polite to others online— stop and think about how your behaviour will affect them.

Tips

- Treat other people the way you would like to be treated. Avoid using bad language and don't say things to someone to make them feel bad.

- Learn about the 'netiquette' of being online. What's considered okay to do and say and what isn't? For example, if you type a message to someone in UPPER CASE they may think you are shouting at them.

- If someone says something rude or something that makes you feel uncomfortable, don't respond. Leave the chat room or forum straight away.

- Tell your parents or another adult you trust if you read upsetting language, or see nasty pictures or something scary.

Playing online games

Playing games online and using consoles or games on a computer can be great fun, but you need to be careful about how much you play and whom you play with. It is important that if you chat with other gamers you protect your privacy and don't share personal or private information. If you are unsure whether a game is suitable, ask your parents or a trusted adult to check its classification and reviews for you.

Tips

- If another player is behaving badly or making you uncomfortable, block them from your players list. You may also be able to report them to the game site operator.

- Limit your game play time so you can still do other things like homework, jobs around the house and hanging out with your friends.
- Keep personal details private.
- Remember to make time offline for your friends, your favourite sports and other activities.

Bullying

The same rules apply online as in the 'real world' about how to treat other people. Unfortunately, people don't always treat each other well online, and you, or a friend, may find that you are the target of bullying. You might be teased or have rumours spread about you online, receive nasty messages or even threats. It can happen in school, or out of it, any hour of the day, from people you know, and sometimes people you don't know. It can leave you feeling unsafe and alone. No-one has the right to bully another person. At its most serious, bullying is illegal and can be investigated by the police.

Tips

- Ignore it. Don't respond to the bully. If they don't get a response they may get bored and go away.
- Block the person. This will stop you seeing messages or texts from a particular person.
- Tell someone. Tell your mum or dad, or another adult you trust. Keep the evidence. This can be useful in tracking the bully down. Save texts, emails, online conversations or voice- mails as proof.
- Report it to:
  - your school—they should have policies in place about bullying.
  - your ISP and/or phone provider or the website administrator—there are actions they can take to help.
  - the police—if there is a threat to your safety the police will help.

If a friend is being bullied online

It can be hard to know if your friends are being bullied. They might keep it to themselves. If they are being bullied, you might notice that they may not chat with you online as much, or they suddenly receive lots of SMS messages or are unhappy after they have been on the computer or checked their phone messages. They may stop hanging around with friends or have lost interest in school or social activities.

Help stop bullying

1. Stand up and speak out! If you see or know about bullying happening to a friend, support them and report it. You'd want them to do the same for you.

2. Don't forward messages or pictures that may hurt or be upsetting to someone. Even though you may not have started it, you will be seen to be part of the bullying cycle.

3. Remember to treat others as you would like to be treated when communicating online.

Your digital footprint

It's great to share things online with your friends. Part of the fun of sharing videos, images and other content, is that lots of people can view and respond. Remember that others whom you don't know may also view what you share with your friends. They may also be able to look at it for years to come. Everything you post adds up to your digital footprint and, once it's online, it could be there forever. So think before you post.

Tips

1. Keep your personal details private. Use an appropriate nickname instead of your real name. Ask your parents before giving anyone on the Internet your name, address, phone number or any other personal details.

2. Don't share your username or password with anyone.

3. Think before you hit send or post. Once posted, it can be content difficult to remove content.

4. Don't post anything you don't want others to know or find out about you - or that you wouldn't say to them face to face.

5. Remember that private images and videos you send to friends or pose of a social networking sire may be passed on to other and uploaded to public areas.

6. Be respectful of other people's content that you post or share. For example, a photo that your friend took is their property, not yours. You should post it online only if you have their permission and make a note about where you got it from.

Offensive or illegal content

When you are surfing the web you may come across websites, photos, text or other material that makes you feel uncomfortable or upset. There are some easy ways to handle these situations.

Tips

1. Tell your parents or another trusted adult if you come across material that upsets you.

2. Know how to 'escape' from a website if an Internet search takes you to an unpleasant or nasty website. Hit control-alt-delete if the site will not allow you to exit.

3. If a website looks suspicious or has a warning page for people under 18 years, leave immediately. Some sites are not meant for kids.

4. Check with your parents that your search engine is set to block material that is meant for adults.

5. Ask your parents to install internet filter software to block bad sites.

6. Ask your parents to help you find safe and fun sites to use and bookmark for later.

Guidelines for the age group 13 years and above

Huge number of young people in this age group use social network sites, online games and Instant Messenger applications. Going online is not just something they do occasionally or for fun. For many it is an integral part of their daily lives. It's how they stay in touch with and communicate with their friends, how they organize large parts of their social lives and school work. Here you will find information on how to be safe using these online platforms as well as insight into what you can do to help create a safe and positive online space for you and your friends.

Harmful and illegal content

Curiosity, interests, and a desire to learn new things and explore new facets of knowledge: the Internet is a great tool to satisfy such needs. But the Internet is an open world in which everyone is free to circulate news or almost anything else. It contains an infinite amount of information, so vast in scope that it is easy to get lost or run into untruths and material not appropriate to your needs or age. We are referring to sites that, for example, promote racial hatred or incite violence, sites that could lead you to come across pornographic or child abuse material and sites that can lead you to self-harm. This can occur in a purely accidental way, as in the case of searches on completely different subjects, through e-mailing, P2P programmes, forums, chat rooms and, more generally, through the many channels involved in social networking.

Therefore

1. Before starting a search you should have a clear idea of what you are looking for;

2. In order to narrow things down you can use advanced search functions or directories, that is, the thematic categories that most search engines provide (i.e., for sports, health, cinema, etc.);

3. Put your critical sense to work and try to determine whether the site is trustworthy: When you access the site do other pages begin to automatically open? Are you able to find out who owns the site? Is it easy to contact the owner? Can you tell who wrote the page or particular article you are viewing? (You can always do another search to find out more about the author and/

or owner). Make sure you have written the website address correctly; there are some sites that use a name similar to another to take advantage of possible incorrect typing. Is the site's text spelt correctly or are there grammatical errors? Are there dates included that can indicate whether the site has been updated? Are there any legal notes (regarding, for example, privacy)?

4. If, while surfing online, you come across sites containing violent, self-harm, racist, illegal or child abuse materials don't forget that these sites can be reported to the police or a hotline. Try to find out to whom you can send these reports in your country; your parents or another adult you trust can also help you in filing a report. You should also talk to someone about what

happened and any feelings you may still have about the occurrence/experience;

5. Contents (images, videos, etc.) that are found on the web relating to sex can often be of a pornographic nature and convey sexual material in a typically adult manner with sentiments that are not appropriate to your age group.

What is grooming?

The Internet and mobile phones can potentially be used by abusive adults to make contact with boys and girls. This happens particularly through SMS and MMS messaging, chat rooms, Instant Messaging programmes, newsgroups, forums, online games, and, more generally, through all the social networking spaces, where it is possible to obtain information on users' ages, sex and more, through the profiles they've compiled.

Sexual predators use the Internet to contact children and young people for sexual purposes, often using a technique known as "grooming". This involves gaining the child's or young person's confidence by appealing to his or her interests. These predators are highly manipulative people. They often introduce sexual topics, photos and explicit language to raise sexual awareness and get their intended victims to drop their guard. Gifts, money and even tickets for transportation are sometimes used to persuade and lure the child to a place where the predator can sexually exploit him or her. These encounters may even be photographed or video- taped, or if a meeting does not take place in the real world the predator might persuade the child to make sexual images of themselves or their friends or take part in sexual activity using a web cam to broadcast it.

Many children and young people who get drawn into these kinds of predatory relationships will lack a certain level of emotional maturity or have low self-esteem that can make them susceptible to this kind of manipulation and intimidation. They may also be hesitant to tell adults about their encounters for fear of embarrassment or of losing access to the Internet. In some cases they are threatened by predators and told to keep the relationship or what happened a secret.

For this reason:

- It is essential that you be aware of this risk, and that not everyone online is who he/she claims to be. Online seducers can often pretend to be your age in order to create an atmosphere of familiarity and trust that could lead to an offline meeting and possible abuse;

http://Bullying...

- Protecting your personal data is important; in the real world, you would never give out such details and you'd never tell people you don't know about your private matters. Even if a nice virtual friendship has been formed, that might seem like it could lead to something more, it is important to remember that you don't always know who is really at the other end of the computer;

- In order to enter a chat room, forum, or more generally, a social network, you often have to compile a personal profile, inserting information that can be detailed to varying degrees. In such cases, it is essential to be cautious about inserting identifiable or traceable data (name and surname, address, the name of your school, mobile phone numbers, e-mail address, etc.). Such details can become accessible to anyone, and it is therefore advisable to create an identity for yourself, using nicknames or aliases and fictional images or avatars, and not provide any detailed personal information;

- When you are curious about your sexuality or your more intimate feelings, remember that the Internet can sometimes be a source of really good advice and information but very often it is better to try to find a way to discuss these things with people who you already know and trust in real life.

- If attempts at allurement or awkward situations should occur, it is important to find someone to speak to, an adult or friend; Internet service providers will also often allow users to report incidents by clicking on "report" or "notify", in order to report the abuse. Alternatively, you can turn directly to the police.

It is also advisable to save e-mails and chat room text, SMS or MMS messages (using "messages inbox", for example), as they can be provided as evidence to the police.

Sexting

Sexting is the sending and receiving of text, photo or video messages of children and young people that are inappropriate and sexually explicit. These images are mostly self generated and shared through mobile phone MMS, Skype and social networking sites where images can be posted and shared (such as Facebook, Twitter, Tumblr, Flickr, YouTube, Instagram, Snapchat etc.)[50] According to a recent survey, about 20 percent of teen boys and girls have sent such messages.[51] Young people may also call it cybersex or sending a nudie, picture or selfie.[52] Most young people do not see 'sexting' as a problem. Many consider it as flirting and are reluctant to talk to adults about it because they are afraid of being judged or having their phones and gadgets taken away.

---

50   So you got naked online. Available at https://esafety.gov.au/~/media/cesc/documents/sygno-english-brochure-pdf-so-you-got-naked-online.pdf (Accessed 3 November 2015)

51   https://www.aap.org/en-us/about-the-aap/aap-press-room/news-features-and-safety-tips/pages/Talking-to-Kids-and-Teens-About-Social-Media-and-Sexting.aspx#sthash.TcXDRfUF.dpuf (Accessed 3 November 2015)

52   http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/ (Accessed 3 November 2015)

Sexting may be considered harmless but there are several risks. Taking, sharing or receiving an image, even voluntarily, can have a long-lasting negative impact. Young people can become vulnerable to blackmail, bullying, unwanted attention and emotional distress. Moreover sexting is illegal. By sending an explicit image, a young person is producing and distributing child abuse images and risks being prosecuted, even if the picture is taken and shared with their permission. It's easy to send a photo or message but the sender has no control about how it's passed on.

When images are stored or shared online they become public. They can be deleted on social media or may only last a few seconds on apps like Snapchat, but images can still be saved or copied by others. These images may never be completely removed and could be found in the future, for example when applying for jobs or university.[53] A study finds that about 90% of self-generated sexually explicit photos and videos by young people are taken from its original upload source and put somewhere else.[54]

It is important to be aware that sexting is not a harmless activity and can have serious consequences. Here are some ways to take action and stay in control[55]:

- If someone is pressurizing you to send a sexually explicit picture of you, ask them to stop. Just don't reply at all and hopefully they'll get the hint. But if they're still bothering you or making you feel upset it's okay to block them - even if it's just for a bit. It is wrong for anyone to be pressuring you in this way.

- If an adult has been making you feel uncomfortable by asking you to send them images, you can report them. If an adult does this it is called online grooming. (You can read more about grooming in the section above.) If you are under 18, they are breaking the law.

- If you have sent a picture or video you regret to a friend, someone you met online or your girlfriend/boyfriend ask them to delete it immediately. If you have received a sexually explicit photo, you should delete it immediately too. Remember if you send it on, you are distributing pornography - and you could get into trouble with the police.

- If your picture is posted online then un-tag yourself and report it to the website where it is posted so it can be removed.

It's important to know that making a report doesn't mean the content will definitely be removed. Most websites have a set of rules - 'Terms of Use' - which they expect people using their site to obey. Websites will only take content down if they break these rules. If you want to have something taken down from a site you should check

to see if it breaks one of their rules. Facebook calls their rules 'Community Standards', YouTube's rules are called 'Community Guidelines' and other sites

53 http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/ (Accessed 3 November 2015)

54 https://www.iwf.org.uk/resources/iwfresearch (Accessed 10 November 2015)

55 Adapted from https://esafety.gov.au/esafety-information/esafety-issues/sexting (Accessed 10 November 2015)

like Tumblr, Twitter and Instagram have their own sets of rules and ways to report. Before using any website you should read them to learn what is, and what isn't, acceptable on the site. You should also learn how to report content to the site.[56]

If you have been affected by sexting it is important to tell someone. Talk your parent, teacher or another adult that you trust so they might be able to get you the support that you really need. Sharing with a trusted friend may help too.

Bullying

Through services such as e-mail, forums, chat rooms, blogs, Instant Messaging programmes, SMS and MMS, and video cameras, it is possible to keep in touch with old friends or make new ones in real time and in all parts of the world and to exchange ideas, play games, carry out research, etc. Although most of these services and the ways they are used are positive, in some cases these same tools can be used to offend, deride, defame and annoy Internet users; and furthermore, violent or offensive off-line behaviour becomes magnified when filmed with mobile phones and exchanged or posted on the Net.

What is bullying? Bullying is the act of intentionally causing harm to another person through verbal harassment, physical assault or other more subtle methods of coercion such as manipulation. In everyday language bullying often describes a form of harassment perpetrated by an abuser who possesses more physical and/or social power and dominance than the victim. The victim of bullying is sometimes referred to as a target. The harassment can be verbal, physical and/or emotional. (www. wikipedia.org)

Very often bullying takes place in schools or local neighbourhoods. Unfortunately, there are increasing numbers of bullies and real forms of bullying online, ranging from offensive websites to harassing text messages, and sending unwanted photos via mobile phones and so on. This particular form of bullying – which can possibly offend and hurt someone without necessarily involving any physical contact – can have just as painful consequences as that of traditional forms of bullying. In United States, about 24% of teens reported being bullied online in 2014[57]. In Europe, 15% of children and young people reported online bullying in 2015[58]. Other studies in

Europe show that cyberbullying is on the rise. Among 13-14 year-olds, the rate of cyberbullying has increased from 8% to 15% in four years (2010-2014)[59].

For this reason it is important that you know that this phenomenon exists and that you are aware of the different forms it can take and what can be done to avoid becoming a victim:

---

56 http://www.thinkuknow.co.uk/14_plus/help/Contact-social-sites/ (Accessed 3 November 2015)

57 Cox 2014 Teen Internet Safety Survey, Available at http://www.cox.com/wcm/en/aboutus/datasheet/takecharge/tween-internet-safety-survey.pdf (Accessed on 26 November 2015)

58 INSAFE and INHOPE helpline data, available at http://helplines.betterinternetforkids.eu/# (Accessed 26 November 2015)

59 European Schoolnet, Bullying in Schools, A summary of research and anti-bullying initiatives, 2015 Available at http://files.eun.org/enable/assets/downloads/Review%20of%20bullying%20and%20cyber%20bullying%20summary%20report.pdf (Accessed 16 November 2015)

- Do not circulate your personal data thoughtlessly, as this could make you easily identifiable and more prone to acts of bullying and intimidation by others your own age;

- Once information is posted online it is out of your control and available to anyone and open to any sort of use. You need to be completely clear on this concept; what may seem like an innocent joke could wind up having very irritating and hurtful consequences for others;

- It is important to refrain from reacting to provocations received via SMS, MMS, and instant messages, in offensive or defamatory e-mails, in chat rooms or during online encounters with other users. Instead you need to employ certain strategies that can exclude or limit the actions of those attempting to provoke you such as:

  o Many games allow for the exclusion of undesirable (or unwanted users);

  o When chat rooms are monitored, it is possible to save the offending text from the chat and report it to the monitor;

  o Abuses can be reported to service providers or, in the case of abuse via mobile phones, the report can be sent to the mobile phone company;

  o In the more serious cases, such as cases involving physical threats, it is advis- able that the police also be informed;

  o It is possible to trace the e-mail account from which the offensive message was sent, but practically impossible to prove who actually used it to send the message. The online bully could also hack into someone else's account and use it for his/her offensive behaviour and therefore letting the blame fall on the unfortunate person whose e-mail account was wrongfully used;

  o Most e-mail programmes offer filters to block unwanted incoming e-mails.

- Many instant messaging programmes offer the possibility of creating a list of names that users can choose to block. In this way, you can prevent unwanted people from making contact with you.

An Instant Messaging (IM) system lets you know when one of your known and approved contacts is online and, at that point, you can begin a chat session with the person you feel like talking with; there are quite a number of different IM systems, such as Windows Live Messenger, ICQ, AOL Messenger, Yahoo Messenger! Bullies know which are the most popular among youngsters and make use of them for their own purposes such as flaming, or provoking an online fight. Conversations or fights that break out online can, at times, have after-effects that drag on at school or other places offline.

In all cases remember that it is important to tell someone about what is happening if you ever feel at all uncomfortable or threatened.

Tell your parents, a teacher or someone within the school staff you feel you can trust. Even telling your friends could be helpful.

You can also report to the service provider or mobile operator, even to the police if it is serious. Remember to save the evidence

of the bullying, as this will be really important when you tell someone.

Bullying is not acceptable either in an online or an offline environment. In many countries there are national or local organizations that you can turn to for help. In some countries, such as Canada, 'cyber-bullying' is considered an actual criminal act. In most countries it is a criminal offence to threaten someone or to harass or stalk them, whether in real life or online.

An interesting fact: the term bully originally had a very different meaning from the one it has today - in fact, 500 years ago it meant "friend" or "family member" – how things have changed!

Defend your privacy: Nowadays, setting up a blog or a personal website, is relatively simple. In order to join a chat room, forum or more generally, a social network, you must first put together a personal profile that includes more or less detailed types of information. Different sites have different rules. Before you enter any information about yourself into a site's database or membership records, check how the information might be used, whether or not some or all of it will be published, and if so where. If you feel uncomfortable with the amount of information being asked of you, if you do not really know or trust the site, don't provide it. Look for another or similar service which asks for less information or promises to treat your information more carefully.

Wherever possible it is advisable to create an identity (or alias) by using an invented nickname and not add anything else. Above all it is important for you to have a clear understanding of what may be and what is best not to share with others. What goes online can quickly go beyond your control and be at anyone's disposal for any possible use:

- Whenever you need to divulge your personal data make sure that whoever is requesting information about you is authentic and serious and also remember that before giving data regarding your friends you need to first inform them and have their permission because they may not be happy about having their e-mail addresses or other information about them passed on to others;

- You may not be obliged to provide all of the information requested of you and you should insert only the types of data that are strictly required. In any event, it is always best to find out as much as possible about the person, service or company you are dealing with before providing your data. In particular check to see if the site asking for the data proposes to send you any advertising material, or if they propose to pass on your details to any other companies. If you don't want them to do either or both of those things, tick the relevant boxes. If they don't offer you an option you really should think about not using the service at all. Send personal photos and videos only to those you actually know, your image constitutes personal data and you need to make sure it is not circulated thoughtlessly. The same goes for images of others. Keep in mind that it is practically impossible to determine where an online image can end up; before filming or photographing someone you should always ask for their permission.

- When you need to register for a particular service, try to employ a few simple devices: for example, use

a password that would be hard to figure out so that no one else can guess it and get into your account; use a complex e-mail address, possibly with both numbers and letters (e.g. mrx- 3wec97@... . com) so it be- comes more difficult to guess by spammers or unknown people who might want to send you unwanted mail; make sure your anti-spam service (for incoming e-mails) and anti-virus controls (for e-mail attachments) are activated and continuously updated; use two e-mail addresses, one which is strictly personal and for correspondence with only your real life contacts (friends, relatives, and such), and another to be inserted in all those online registration forms that ask for personal data (user profiles, competition announcements, online games, etc.) that

you already know could be accessed by strangers.

• Do not open email attachments from sources you do not know or programmes you do not know the possible effects of, they could be a Key Logger (capable of recording all the keys being punched on the keyboard, enabling them to find out passwords, numeric codes, credit card numbers etc.), E- Grabber (capable of gaining access to all the e-mail addresses stored on the victim's PC), or Info Grabber (capable of extracting information such as the various Registration Keys of a PC's most important programmes). Without your knowledge these programmes can send over the Internet all the information these programmes pick up to unknown persons.

• Only engage in activities that you feel you are absolutely sure about. If you "smell something fishy", something that's not quite right, that doesn't totally convince you, or you think is being unjustly charged for, then your best move is to leave it alone. You have the right to criticise and question what you come across while online. Remember things are not always as they appear.

Respect copyright

What's great about the Web is the infinite possibilities of finding and accessing all kinds of materials through search engines and they can be downloaded either free of charge or paid for through your PC or mobile phone, and then used offline. Not everything found online can be used as you might wish; a lot of content is protected by copyright law or entitlement rights.

• Peer to Peer (P2P) software enables one to share and exchange one's files directly with other Internet users, without any extra connection costs. Music, films, videos, and games are among the materials that are most sought after and downloaded by youngsters, but they are often covered by copyright provisions and protected by law. Unauthorized downloading and distribution of copyright-protected content

• is a crime in most countries and punishable by law. It is also possible for your involvement in illegal downloading of copy-righted material to be traced. This has led, for example, to a child's parents being sent an enormous bill to cover the cost of the material downloaded and if the family refuse to pay

the bill other forms of legal action can be taken. Some countries are considering banning people from using the Internet if they are caught persistently using it to obtain unauthorised access to copyrighted material. In addition, when using other people's work, like articles or dissertations, remember to quote the sources appropriately. If you fail to do so it will be classified as plagiarism and that can cause you a great deal of trouble.

Remember

- You are free to use, modify and distribute freeware programmes that are not copyright-protected;
- Some software are, on the other hand, shareware, and therefore free for a specific trial period;
- Your privacy and your PC

could be harmed by viruses or other "malware". It is therefore always best to install and continuously update protection systems such as anti-virus, anti-dialer software and a firewall. Always make sure to read the guide relating to the programme you are using to avoid making the errors that are listed below;

- Copyright protected material is generally indicated by standard wording, such as "all rights reserved" or other similar phrasings; in cases where this is not evident, it is nonetheless best not to take any risks;
- The Peer to Peer (P2P) programmes you use to share and download files also carry certain risks. One must have a very thorough understanding of them to be able to use them without running any security risks:

  o You may not always end up downloading what you intended to download: different types of content may be concealed behind the title of a song or video. In the worst cases, for example, it might contain child abuse images. Examine your particular programme guide to find out how you can detect fake files and only go to sources you know are trustworthy: ask your friends to tell you which sources to use and which to avoid;

  o Before opening a downloaded file make sure to scan it for viruses; another quite frequent risk is in fact that a downloaded file might contain viruses and spyware that can put PCs, personal data and privacy at risk;

  o Do not share your entire hard disk: check your configurations to ensure that you have shared only those folders you wanted to share and remember that sharing files protected by copyright is a crime.

Online commerce

You can purchase products online or by using a mobile phone. Purchases can be made by credit card or, in the case of mobile phones, by debiting the credit on the mobile phone subscription. There are also online spaces devoted to exchanges and purchases of all sorts of products, at very competitive prices.

One of the fundamental difference between online and traditional commerce lies with the difficulty in identifying who is at the other end of the exchange and the risk of fraud that may lie just around the corner. One of

the most widespread risks is that of "phishing". This happens when people respond to fake emails, spam, which usually appear to come from a reputable source e.g. a bank or credit card company. They will ask you to enter a lot of personal information e.g. bank account details, passwords, date of birth and so on, which they will then misuse.

An additional complication with online commerce concerns the sale of products or services that are age restricted in some way. For example, in many countries it is illegal for vendors to sell or provide alcohol or tobacco to legal minors. Gambling is also generally limited to people over a certain age. Yet in the online environment it can be very hard for the vendor to determine the age of the person proposing to make the purchase or acquire the service. All that many companies do is ask the person to check a box to confirm they meet the minimum age requirement.

Some companies in a number of countries are beginning to deploy age verification systems linked to their purchasing procedures, but this is still a very new and limited technology, however it is a grow-ing, practice. Buying age restricted products online, and telling lies about your age in order to do so means you could be committing a criminal offence and so could the vendor. You could forfeit the goods and you could end up with a criminal record, so don't do it.

There are, in any case, a series of tactics that can help you reduce the risks and enable you to make use of the convenient opportunities offered by online commerce:

- Take great care in choosing the sites that you want to make purchases from and ensure their credibility. Gather as much information as you can about the site in question, such as name, address, telephone number and head office of the company, description of the contract's general conditions and, in particular, how to withdraw from the purchase; also find out about the protection and management of personal data and payment security; and compare prices, looking for the same item on other sites;

- Prepaid credit cards, or ones that can be topped up, come with spending limits and can help avoid unpleasant surprises.

- Before you buy anything online, make sure the site uses a secure system for transactions so as to prevent, for example, "sniffing", which is a means of capturing data during transmission. Even though many sites incorporate systems that counter the interception of data in transit, your details could still be stolen if someone hacks into the server of the company where your credit card details have been stored. Clearly, by choosing other modes of payment you can avoid the possibility of someone stealing your credit card number.

- If you receive an unsolicited e-mail offering you an incredible deal, it is highly likely that it is fraudulent;

- If something looks too good to be true, it most probably is, and it would be best to forget about it.

- In the case of purchases made by mobile phones for which a credit card is not re-quired, verify what the costs of the services actually are, the service's conditions of agreement and how one can back out.

4.

Conclusions

By keeping these basic rules in mind, you will be able to steer clear of the majority of the pitfalls you can encounter online. Should you encounter unpleasant or disturbing experiences, make sure you talk to a trusted source. Remember, you have the right to be protected as well as the responsibility to act appropriately, offline as well as online.

Sources for Further Reading & Inspiration

United Nation's Convention of the Rights of the Child
http://www.unicef.org/crc/

WSIS Outcomes
http://www.itu.int/wsis

WSIS+10 High Level Event Outcome Documents
http://www.itu.int/net/wsis/implementation/2014/forum/inc/doc/outcome/362828V2E.pdf

ITU's activities on cybersecurity
http://www.itu.int/cybersecurity

Child Online Protection (COP) Initiative
http://www.itu.int/cop

Imagine Your Future – a prediction of how the future will be http://www.elon.edu/e-web/predictions/kidzone/yourfuture.xhtml#kids%27%20 predictions

The Internet Big Picture - World Internet Users and Population Stats http://www.internetworld-stats.com/stats.htm

Child-friendly version of 'A World Fit for Children'
http://www.unicef.org/ceecis/child_friendly_ssoc_outcome.pdf

Opinion polls: What young people think
http://www.unicef.org/polls

Connect Safely is for parents, teens, educators, advocates - everyone engaged in and interested in the impact of the social Web
http://www.connectsafely.org/

Children and Adolescents Statement at World Congress III Against Sexual Exploitation
http://www.unicef.org/brazil/pt/br_IIIWC_En.pdf

The Children and Young Person's Global Online Charter http://www.iyac.net/children/index.htm

A number of Childnet's resources for young people
http://www.childnet-int.org/young-people/

Internet safety information (access to sites in different languages)
http://www.saferinternet.org/ww/en/pub/insafe/index.htm
http://www.getnetwise.org/

Appendix 1

Parent Contract

I know that the Internet can be a wonderful place for my kids to visit. I also know that I must do my part to help keep them safe on their visits. Under- standing that my kids can help me, I agree to follow these rules:

1. I will get to know the services and websites my child uses.

2. I will set reasonable rules and guidelines for computer use by my children and I will discuss these rules and post them near the computer as a reminder.

3. I will not overreact if my child tells me about something "bad" he or she finds or does on the Internet.

4. I will try to get to know my child's "online friends" and Buddy List contacts just as I try to get to know his or her other friends.

5. I will try to provide close support and supervision of my younger children's use of the Internet, for example by trying to keep their computer in a family area.

6. I will report suspicious and illegal activity and sites to the proper authorities.

7. I will make or find a list of recommended sites for children.

8. I will frequently check to see where my kids have visited on the Internet.

9. I will seek options for filtering and blocking inappropriate Internet material from my children.

10. I will talk to my kids about their online explorations and take online adventures with them as often as I can.

I agree to the above.

Parent signature(s)

_____

Date

_____

I understand that my parents have agreed to live by these rules and I agree to help my parents explore the Internet with me.

Child signature

_____

Date

_____

Child's Contract

I know that the Internet can be a wonderful place to visit. I also know that it is important for me to follow rules that will keep me safe on my visits. I agree to the following rules:

1. Wherever possible I will choose a safe and sensible screen name for myself that will not broadcast any personal information about my family or me.

2. I will keep all of my passwords private.

3. I will discuss with my parents all of the different programmes and applications I use on my computer and on the Internet, and talk to them about the sites I visit. Before I download or load a new programme or join a new site I will check with my parents first to make sure they approve.

4. When considering signing up to a new online service I will avoid those which demand too much personal information and try to opt for those which ask for less.

5. I will always take steps to find out what personal information about me will be published by the service by default in my profile and will always opt for the maximum degree of privacy.

6. I will not share my personal information, or that of my parents or any other family member, in any way, shape or form, online or with someone I meet online. This includes, but is not limited to name, address, telephone number, age or school name.

7. I will treat others the way I want to be treated.

8. I will use good manners when I'm online, including good language and respect. I will not pick fights or use threatening or mean words.

9. I will make my own personal safety my priority, since I know there are some people who might be online and pretend to be someone they're not.

10. I will be honest with my parents about people I meet online and will tell them, without always being asked, about these people. I won't answer any e-mails or instant messages from anyone my parents have not approved.

11. If I see or read things that are bad, icky or mean, I will log off and tell my parents so they can try to make sure it never happens again.

12. I will tell my parents if I receive pictures, links to bad sites, e-mail or instant messages with bad language or if I'm in a chat room where people are using swear words or mean and hateful language.

13. I will not send anything in the post to anyone I've met online, without my parents' okay. If I get something in the post from someone I've met online, I'll tell my parents immediately (because that means they have my private information).

14. I will not do anything online that someone asks me to if it makes me feel uncomfortable, especially if I know it's something my parents would not be happy about or approve of.

15. I will not call, write a snail mail or meet in person anyone who I've met online without my parents' approval or without a trusted adult coming with me.

16. I understand my parents will supervise my time online and may use software to monitor or limit where I go online. They're doing this because they love me and want to protect me.

I will teach my parents more about the Internet so we can have fun together and learn cool new things.

I agree to the above.

Child signature

_____

Date

_____

I promise to protect my child's safety online by making sure these rules are followed. If my child encounters unsafe situations and tells me, I will handle each situation with maturity and good sense, without blaming anyone, and will calmly work through it with my child to ensure their safer Internet experiences in the future.

Parent signature(s)

_____

Date

_____

With the support of: