eNACSO European NGO Alliance for Child Safety Online

A Digital Manifesto

- an agenda for change

Co-funded by the European Union

Contents

1 Foreword

The European NGO Alliance for Child Safety Online – eNACSO - is a network dedicated to making the internet and associated technologies safer for children and young people.

Our members are leading children's rights and child protection NGOs from across the European Union.

eNACSO promotes and supports actions at national, European and international level. Our work is based on the 1989 UN Convention on the Rights of the Child[1] and its Optional Protocol on the sale of children, child prostitution and child pornography.

This manifesto presents eNACSO's recommendations to governments, industry and other stakeholders on how to create a safer online environment for children and young people.

If you would like any further information about anything discussed in this document or about eNACSO's other work, please do not hesitate to get in touch.

On behalf of eNACSO

John Carr

John Carr

Executive Board Member

info@enacso.eu

www.enacso.eu

November, 2009

[1] www.unhchr.ch/html/menu3/b/k2crc.htm

2 eNACSO Members (Nov 2009)

action innocence	**BELGIUM** **FRANCE**
ecpat	**AUSTRIA** **HOLLAND**
Innocence in danger	**GERMANY**
ISPCC ALWAYS HERE FOR CHILDREN	**IRELAND**
KÉK VONAL Gyermekkrizis Alapitvány	**HUNGARY**
Lastekaitse Liit Estonian Union for Child Welfare	**ESTONIA**
NOBODY'S CHILDREN FOUNDATION	**POLAND**
NSPCC Cruelty to children must stop. FULL STOP.	**UNITED KINGDOM**
NADACE NAŠE DÍTĚ · OUR CHILD · NOTRE ENFANT · UNSER KIND	**CZECH REPUBLIC**
protegeles.com	**SPAIN**
Save the Children	**DENMARK** **FINLAND** **ITALY**
Mr. John Carr	**UNITED KINGDOM**

3 Executive Summary

Many different kinds of societies are benefiting from the emergence of the internet as a mass, consumer technology. Children and young people are a major constituency of users. The internet's ability to provide a platform for learning, creativity, connectivity and games is at the heart both of its value and its attraction to the hundreds of millions of children and young people worldwide who now use it daily.

However, it is also important to recognize that the internet has brought with it a number of unforeseen, unwanted and unintended consequences. Some of these can put children and young people at risk of significant harm. For example new types of bullying and new forms of sexual solicitation of children and young people have been facilitated by the internet. The number of child abuse images[2] in circulation has hugely increased.

Governments have an overriding duty to provide for the safety and well being of all children and young people within their jurisdiction but to do this effectively they must work in partnership with others. Making the internet and associated technologies safer for children and young people is a shared responsibility, just as it is in many other environments.

Children and young people themselves, parents, teachers, law enforcement agencies and high tech companies, all have a critical part to play. Effective education and awareness initiatives are central. Technical solutions can also make a vital contribution.

International organizations have a key leadership and supportive role both to encourage and promote the development of more effective solutions and, perhaps above all, to help countries that are just beginning to grapple with the challenges of online child safety. We can all learn from the experience of others.

Other recommendations include

Online child abuse and child abuse images

- The harmonization and modernization of national laws and police procedures for dealing with online child abuse and online child abuse images needs to be given a high priority

- We need to achieve a higher rate of detection, location and rescue of children and young people who appear in child abuse images on the internet

- Faster ways need to be found to remove child abuse images from the internet or block access to them

- ICANN must become more proactive in the fight against child abuse images

- Improved training and support for professionals working in this area is essential

[2] Throughout this document the term "child abuse images" is used rather than "child pornography" because this more accurately reflects the nature of the content.

Advertising, E Commerce, Privacy and Data Protection

- Children and young people need protection from commercial practices which take advantage of or are careless about their naïveté

Location services and mobiles

- Technology companies and the mobile phone industry need to establish strong safeguards in relation to the emergence of new types of location services and tracking technologies

Social networking sites and legal barriers

- Social networking and other sites that accommodate user generated content should play an active role in monitoring that content, particularly pictures and videos
- The "mere conduit" laws should be revised so that legal liability can only arise if a company has actual knowledge of an unlawful item and then intentionally fails to remove it or fails to act expeditiously
- Clear routes should be available to enable all internet users to report abuse to the appropriate agency

Future of self-regulation and support for NGOs in the policy making processes

- More resources must be found for NGOs in order to enable them to make an optimal contribution to the multi stakeholder policy making processes
- To maintain public confidence in self-regulation as a mechanism for policy making, convincing evidence of an improvement in online child safety is required

4 Children, young people and the internet: an overview

The internet[3] has become an enormously important technology in the modern world. eNACSO strongly believes in the potential of the internet to enrich and empower children and young people in many different ways. eNACSO actively promotes safe and equal access to the benefits of the internet for all children and young people everywhere.

Children and young people are a major constituency of users on the internet. Its ability to provide a platform for games, connectivity and creativity is an undoubted part of the value and attraction to the hundreds of millions of children and young people worldwide who now use it daily. They will soon be joined by hundreds of millions more.

4.1 A positive force in the world

For most of the time for most of the children and young people who use it, the internet will be an upbeat and positive place. That is one of the reasons why whenever we talk to children and young people about the internet and the new technologies it is essential to maintain the same upbeat and positive attitude. If the only way we ever discuss the internet is in terms of it being a worry and a threat we will simply be communicating to children and young people that we don't understand it, then why should they listen? The aim should be to help children and young people to have a realistic understanding of the internet's hazards and help them deal with those hazards or navigate around them, not put them off it.

4.2 Striking the right balance

This approach means we have to acknowledge that at different times any and all children and young people can experience the internet and associated digital technologies in ways which might be distressing or harmful, or both.

Some commercial companies and other organizations exploit or are careless about children and young people's innocence and can compromise their right to privacy and safety. The emergence of new location and tracking technologies poses particular challenges. Parents and educators need to know how to strike the right balance between, on the one hand, being realistic about the risks but, on the other, not exaggerating them, thereby perhaps discouraging children and young people from using the technology at all. That would be a great loss to the children and young people as individuals, as well as to society as a whole.

[3] There are many ways the internet can be accessed, e.g. via laptop, desktop, notebook-sized or handheld computers, through mobile phones, games consoles, personal digital assistants and TV. Rather than repeat this list throughout this document, unless the text provides otherwise, all of these mechanisms are relevant.

4.3 A question of rights

Children and young people have a legal right to grow up and develop free from sexual or other kinds of exploitation[4]. These rights are guaranteed under international law and have been incorporated into the domestic legislation of every EU Member State. eNACSO's members work with children and young people and their families to identify and articulate how these rights are given effect in the online space.

4.4 Virtual and real worlds becoming more closely aligned

As children and young people increasingly live out significant parts of their lives with and through the new technologies, the nature of the risks they take online have become inextricably entangled with wider aspects of their behaviours.

If it ever was, it is now simply no longer possible to draw neat lines between so called 'internet issues' and 'real world' problems. A tightly maintained consensus within the policy community about some of the earlier problems that were identified with the internet has now given way to a range of broader debates about how children ought to be encouraged to behave. With this widening of the parameters of internet safety debates, the difficulty of reaching or maintaining a consensus has increased.

4.5 Digital divide?

In recent years, and partly to counter some of the criticisms about the impact of new technology, one of the dominant narratives to emerge in the digital space is about how the internet is a liberating tool for children and young people. A great deal of money and power has been put behind the promotion of that idea. Yet for some children and young people the internet clearly fails to deliver on this promise and, even leaving aside questions of risk, they may have a narrow and unrewarding internet experience.

The internet certainly can provide an enormously enriched environment for very many users, particularly younger users, but it could also be contributing to a further widening of pre-existing divisions in society or even be responsible for opening up new ones.[5] It is a divide rooted not only in possessing, or not possessing, the physical means of accessing the internet, it is a divide that is influenced by several other factors.

Professor Sonia Livingstone's research into children and young people's activities online established[6] that an individual's level of media literacy and self-confidence in using the internet will be decisive in determining whether or to what extent that individual benefits from it. For these reasons, in developing policies to address

[4] Conferred by the UN Convention on the Rights of the Child and the Optional Protocol on the sale of children, child prostitution and child pornography.

[5] Similar points have also been made, particularly at the UN and within WSIS, about how at a macro level a new social and economic divide can open up between countries that have, or do not have, large scale access to the new technologies. See http://www.itu.int/wsis/docs/geneva/official/dop.html.

[6] *Drawing conclusions from new media research: reflections and puzzles regarding children's experience of the internet*, LSE, 2006

the digital divide, it is imperative not only to find ways to improve and widen the availability of the physical means of access, but also to focus on improving the media literacy and self-confidence of individual users. Much will depend on the successful delivery of policies that address this aspect.

4.6 The role of governments and international agencies

Clearly national governments have the prime responsibility to act to protect all children and young people within their jurisdiction but to do this they must work in partnership with others. The internet is a global medium. This places a particular onus on international institutions to lead and encourage action at national and international level. The EU[7] has been a pioneer in this field. Its annual "Safer Internet Day", coordinated by INSAFE, in effect has gone global, providing a very valuable focus for education and awareness activities in every major language across all five continents. The ITU[8] is now also spearheading a very important worldwide initiative that is gathering momentum. Perhaps above all international institutions are best placed to help countries that are just beginning to grapple with the challenges of online child safety. We can all learn from the experience of others.

4.7 A multi stakeholder approach is essential

No single agency or interest, public or private, no company or other organization has a monopoly of knowledge or expertise in the field of online safety. Providing a safe environment for children and young people on the internet is a shared responsibility, just as it is a shared responsibility in many other environments.

Children and young people need to be equipped to keep themselves safe online. Parents, guardians and teachers need to be helped to understand how children and young people use the new technologies so they, in turn, can help ensure children and young people get the most out of them but also know how to use them safely.

Schools have a pivotal supporting role to play here. NGOs are also key but they may need some assistance to help develop their capacity to contribute. Partnerships with law enforcement are vital to ensure appropriate messaging is developed and properly integrated into wider education and awareness measures.

Industry is uniquely placed to make a contribution in two ways: firstly by helping all stakeholders to produce and promote effective education and awareness resources as well as producing materials themselves which speak to their own customer base and markets. Secondly, by developing and promoting more and better technical solutions which underpin and reinforce the safety messages.

[7] http://tiny.cc/eusip19

[8] http://tiny.cc/itucop

5 Children's vulnerabilities

While everyone is potentially exposed to the same range of risks and dangers online, children and young people are often particularly vulnerable to some of them. Children and young people are still in a process of developing and learning. This has consequences for their capacity to identify, assess and manage potential hazards.

As children's rights organizations, the principle that children and young people are more vulnerable is core to our perspective and our work on internet safety. It is also embedded in the entire range of child protection and child welfare policies and legislation of many different countries in all parts of the world.

In relation to the internet there are a number of issues about children and young people's vulnerabilities that are of ongoing concern. These may be summarized as follows:

5.1 Content

1. The internet's ability to expose children and young people to legal but age-inappropriate material e.g. adult pornography or very violent imagery.

2. The internet's ability to expose children and young people to different kinds of illegal content e.g. child abuse images

5.2 Contact

3. The internet's ability to expose children and young people to bullying behaviour by or sexual solicitations from adults or other minors.

4. The internet's ability to expose children and young people to harmful online communities such as sites which encourage anorexia, self harm or suicide – as well as sources of political influence espousing violence, hate and political extremism.

5.3 Conduct

5. The internet's ability to facilitate and promote risky sexual interactions between children and young people, including encouraging them to take and post pictures of themselves or others ("sexting") which, aside from being harmful, may also be illegal.

6. The internet's ability to facilitate or encourage children to place in the public domain information about themselves, or post pictures or videos or texts that compromise their personal safety or jeopardize a number of future career options.

7. The internet's ability to expose children and young people to bullying can also allow or promote an environment in which children and young people are encouraged to bully others.

5.4 Commerce

8. The internet's ability to enable children to access or acquire age-inappropriate goods and services, typically goods and services they could not legally obtain on the high street because vendors are required to confirm the buyer's age. Vendors do this by performing a visual age check and, if there is any reasonable doubt about the person's age, they are required to ask for proof or decline the sale.

9. The internet's ability to expose children and young people to scams, identity theft, fraud and similar threats that are economic in nature.

10. The internet's ability to compromise a child or young person's personal safety through inadequate, unclear or unenforceable data protection or privacy laws.

5.5 Addiction

11. The internet's ability to facilitate access to games which can be played over it, or to create alternative environments, where these seem to have encouraged forms of obsessive behaviour or excessive use which may be having a deleterious effect on their health or social skills, or both.

5.6 Societal

12. The internet has the potential to compound and even magnify existing vulnerabilities of particular children and young people, thereby adding to adversities they may face in the real world.

13. The internet may be opening up a new digital divide among children and young people, both in terms of those who have ready and convenient access to it at home, school and elsewhere, and those who do not, as well as between those who are confident and proficient users of it and those who are not. This divide threatens to entrench or widen existing patterns of advantage and disadvantage or perhaps create new divides.

14. At a macro level a digital divide between nations or regions similarly may entrench or widen existing global patterns of disadvantage.

6 Key recommendations

6.1 The need for a comprehensive policy

1. Governments should develop a comprehensive range of policies to address internet safety for children and young people. In developing such a policy it will essential to draw on the expertise and knowledge of all the stakeholders.

2. It is particularly important to produce education and awareness programmes which reach out directly to children and young people. Law enforcement needs to find appropriate ways to integrate their messaging into these programmes.

3. It is also essential to find ways to help parents and teachers to understand the new technologies and how children and young people use them so that they, in turn, can provide help, advice or support.

4. High tech companies have a particular role to play in helping all stakeholders to develop and promote effective educational resources as well as developing materials for use with their own customer base and markets.

5. High tech companies also have a unique role to play in terms of developing technical solutions which can contribute to online child safety.

6.2 International leadership

6. The global nature of the internet places a particular responsibility on international institutions to lead and encourage action at national and international level. Intergovernmental and regionally based initiatives such as the ITU's Child Online Protection initiative and the EU's Safer Internet Programme have a vital role in pushing forward the agenda. International institutions are perhaps best placed to help those countries just beginning to grapple with the challenges of online child safety.

6.3 Online child abuse and child abuse images

7. Laws made before the arrival of the internet may need to be modified to ensure they do not create barriers to the proper safeguarding of children online e.g. modern laws should recognise that a range of sexual offences against children and young people can be committed in remote environments such as the internet. The online sexual solicitation or "grooming" of children is an example and should be outlawed in every country.

8. There is an urgent need to achieve a much greater degree of harmonization of laws and police procedures for combating online crimes against children and young people, including the laws and police procedures for dealing with child abuse images.

9. There should be discussions at an international level with a view to developing faster ways to remove child abuse images from the internet or block access to them.

10. Every country should ensure that within their jurisdiction appropriate steps are taken by online service providers to block access to all internet addresses known to contain or promote access to child abuse images.

11. Hotlines which receive reports about the location of child abuse images on the internet are essential. Every country should have a Hotline which meets the needs of all linguistic groups within its jurisdiction. The quality of the Hotline should meet INHOPE[9] agreed standards.

12. In order to promote the more efficient investigation, removal or blocking of child abuse material worldwide, international and intergovernmental bodies, national governments and others should expedite the creation of a single list of all known child abuse addresses, or a list that is as large as possible, drawing on any and all national lists that are not currently encumbered by local legal constraints. With appropriate security surrounding its deployment, this list should be made available to relevant online service providers, filtering companies and others with a material interest.

13. Governments, law enforcement and industry should begin discussions about how to combat the use of peer-to-peer software for the distribution of child abuse images and how to combat

14. the emergence of other types of closed groups or communities that have the same purpose.

15. The high tech industries should seek ways to prevent the misuse of encryption software and other technologies from facilitating the exchange of child abuse images.

16. Governments should ensure that adequate resources and technical tools are available to law enforcement agencies charged with dealing with child abuse images. They should also sponsor the development of an internationally based investigative unit with a specific remit to focus on the criminal networks behind a high proportion of the trade in child abuse images.

17. Drawing on the technical research currently being funded by the EU's Safer Internet Programme and others, governments should provide more resources to help law enforcement to achieve a higher rate of detection, location and rescue in real life of children who have appeared in child abuse images on the internet.

18. Representations should be made to ICANN with a view to securing a substantial improvement in the regulatory performance of those domain name registries that currently appear to be ineffective in preventing child abuse images from being published under their auspices. ICANN should also be asked to give an undertaking that it will not allow any national or other registries to accept or allow domain names to be registered or maintained which advertise the availability of or promote child abuse images.

[9] https://www.inhope.org/

6.4 Support for professionals and treatment programmes

19. The bodies responsible for the accreditation of police, health, social workers, youth workers, teachers, probation and prison staff, need to ensure that proper recognition is given within their professional qualifications and their professional development programmes to the importance of being able to recognize the manifestations of online abuse in victims, and be familiar with the kinds of abuse engaged in by perpetrators.

20. Governments should ensure that appropriate resources are developed to address the therapeutic needs of children who have been sexually abused where images of that abuse have appeared on the internet.

21. Appropriate assessment and treatment programmes should be available for children displaying inappropriate or aggressive sexual behaviour online.

22. The relevant agencies need to ensure there is sufficient availability and take up of treatment programmes for internet offenders.

6.5 Advertising, e commerce, privacy and data protection

23. Policies and standards need to be developed which protect child and young people from exposure to age inappropriate advertising and age inappropriate commercial activity.

24. Data Protection and Privacy Commissioners should issue clear advice and guidance on the respective rights and responsibilities of all the parties where online data or other transactions involving children and young people are concerned. In particular, the Commissioners should consider setting, or asking for appropriate authority to set, a legally defined minimum age below which verifiable parental consent will always be required in an online environment.

25. Adult products and services should not be advertised on web sites which are primarily used by children and young people, or where substantial numbers of children and young people are known to be regular users. A clear definition of what constitutes a children's website should be formulated and all advertising on such sites should conform to the equivalent or relevant real world advertising standards.

26. Vendors should not be able to avoid or evade laws on the sale of age restricted goods and services e.g. alcohol, tobacco, pornography, gambling, weapons, by making them available over the internet. Appropriate regulations should be developed to govern the online sale of age-restricted goods and services.

27. Regulators need to monitor the development of forms of online payment which are anonymous and could therefore facilitate the illegal purchase of age restricted goods and services, or could facilitate trade in other illegal items e.g. child abuse images.

6.6 Addressing future challenges: the mobile internet and location services

28. Mobile network operators have a special responsibility towards children and young people. They should ensure only appropriate e-commerce activities are available to minors who use their networks. All adult services should be behind an adult bar

29. The mobile phone handset manufacturers should accept a larger role in the ongoing discussions about child safety on the internet with a view to developing safety features that can operate by default and are integrated directly into the handsets. They should also consider developing devices with a much reduced feature set and therefore avoid some of the risks to children and young people that seem to be unavoidably associated with the more sophisticated models.

30. Providers of wifi or other forms of remote internet access should replicate the arrangements currently made by many mobile network operators to restrict the availability of adult sites.

31. The new types of location services and tracking technologies now emerging into the consumer market pose challenges not only in the field of online safety for children and young people, but also in relation to the civil and privacy rights of all citizens. Strong safeguards must be developed to govern their use.

6.7 Social networking sites

32. Social networking sites should have clear and transparent standards to address online child safety, including easy to use procedures to report abuse to the appropriate agency.

33. Social networking sites should have mechanisms which allow them proactively to review content on their site, especially pictures and videos. They should also ensure they review all content reported to them within a clearly specified time period.

34. Independent mechanisms should be developed to monitor and report on the extent to which agreed standards are being observed by social networking sites.

6.8 Removing legal barriers

35. Efforts should be made to clarify the civil and criminal liabilities of online service providers in relation to user-generated content hosted on their sites. In particular, governments should press for an amendment to the E-Commerce Directive and similar “safe harbour” provisions in other jurisdictions to remove any disincentive for companies to police their own sites for fear of attracting liability. The principle should be that for any kind of civil or criminal liability to exist, it is always necessary to show the hosting company had actual knowledge of the unlawful content and deliberately took no action to remove it or failed to act within a reasonable time.

6.9 Self-regulation and support for NGOs in the policy making processes

36. The multi stakeholder approach to policy making ultimately depends on each individual stakeholder having both the will and the means to take part. Typically very many NGOs have the will but too often they lack the resources to allow them to make an optimal contribution. Ways should be found to help NGOs to develop their capacity to engage constructively and in a well-informed and timely way in the multi stakeholder policy making processes, both nationally and internationally.

37. To maintain public confidence in self-regulation as a mechanism for policy making, convincing evidence of an improvement in online child safety is required.

--ooo---