SUBMISSION No. 18

Childnet International response to Joint Select Committee on cyber-safety on cyber safety issues affecting children and young people.

About Childnet

Childnet International is a UK-based charity working domestically and internationally to help make the Internet a great and safe place for children and young people, alongside enabling them to use interactive technologies safely and responsibly.

Childnet focuses on education, awareness and policy and has developed a number of award-winning educational resources in partnership with the UK Government and others, including the award winning Know IT All range of resources and advice on cyberbullying, designed to help young people and parents assess and manage the risks that they may encounter online.

Alongside promoting the opportunities that the Internet and new technologies offer, Childnet is active in carrying out research and engaging in key policy fora alongside the Internet industry and governments. Childnet is an original member of the UK Council for Child Internet Safety (UKCCIS).

Introduction

Childnet's responses to this inquiry are drawn from our daily experience working alongside teachers, parents, children and young people in schools in the UK, and our working in partnership with others across the world, including Australia.

Childnet responded to two inquiries in the UK covering similar subject areas in 2007, The Byron Review on children and new technology[1], and the Culture, Media and Sport Committee's Inquiry on Harmful content on the Internet and in Video Games[2], which may be of interest to the Joint Select Committee.

The online environment in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles)

A review of young Australian's use of online social media was carried out by the Australian Communications and Media Authority (ACMA) and published in the Click and connect reports in July 2009[3]. An additional study (Online risk and safety in a digital environment[4]) carried out by the ACMA provides further information on this area.

Slide from Childnet's presentation for parents shown in schools outreach work.

The internet landscape has evolved dramatically over the past few years, and the opportunities that the internet and accessing internet technologies offers to children and young people are fantastically varied. With the development of the internet, access has increasingly become more fluid. Our weekly contact with children and young people has confirmed that access is no longer restricted to a fixed computer, but that the internet is frequently accessed through mobile phones, hand held gaming devices and gaming consoles. We know from our work with teachers, parents, children and young people in schools that children are making use of these access points and in many cases are using them unsupervised.

[1] www.childnet.com/downloads/byron-review.pdf
[2] www.childnet.com/downloads/080130Response-CMS.pdf
[3] www.acma.gov.au/WEB/STANDARD..PC/pc=PC_311797
[4] www.acma.gov.au/webwr/_assets/main/lib310554/online%20risk_safety_report_2010.pdf

The internet is evermore becoming more portable and private, and also personalized with many websites and services tailoring the content that they offer to the specific user. Very often we have found that parents are not always aware of the ways and means through which their children and young people are accessing the internet, and this is something that we seek to address and communicate in our work with parents.

Mobile phones and 'remote access' can encourage 'spontaneity' of online activity which can act to minimise the thought processes of children and young people engaging online in this way exposing them to more risk than perhaps they would otherwise face, and can also facilitate young people in bypassing any filters or security measures that have been put in place. "*Computers at schools are blocked, but everyone has BlackBerrys so boys swap sex sites at break time*" (Sami, aged 13)[5]. The decrease in age of mobile phone ownership and our experience with schools in the UK tells us that children as young as 5 are interacting with the online environment. We believe that it is important to engage with children at the age when they are first starting to interact with these technologies and forming their behaviours and at Childnet we are increasingly being asked to talk to nurseries and kindergarten aged children about e-safety and staying safe online.

The mobility of access, through mobiles, and wireless access for example, and the challenges that throws up in terms of supervision, fully illustrates the crucial part that education must play in helping to keep children safe and ensure they are safe and responsible users of technology. Children need to be able to make good decisions online, whenever and wherever they are online.

Abuse of children online, particularly cyber-bullying

The contact risks facing children and young people online include grooming and cyberbullying. A growing body of evidence suggests that bullying and harassment are the most frequent threats that young people face online[6], and from the work we undertake with children and young-people, we know that cyber-bullying is one of the risks that they are most worried about[7]. Research undertaken in the UK in 2009 revealed that 30% of 11-16 year olds have experienced some form of cyberbullying, and, 8% of this age group have been persistently cyberbullied.[8] In Australia, the Australian Covert bullying prevalence study of May 2009 highlighted 7-10% incidences of cyberbullying among young people[9], and the Click and Connect reports recorded slightly higher incidences.[10]

The situation in Australia, just as it is in the UK, is that, whichever research statistic you take, we are seeing that Cyberbullying is a feature of many young people's lives.

Other risks that children and young people face online include sexual bullying and sexting (the sending of messages or images with sexual content via mobile phones or the internet). A recent survey in the UK in 2009 by the South West Grid for Learning revealed that around 40% of teens questioned said that they knew friends who had been involved in sexting. Over a quarter, 27%, of respondents said that

---

[5] Aitkenhead, D. (2010) Psychologies: Are teenagers hooked on porn? (online edition: www.psychologies.co.uk/articles/are-teenagers-hooked-on-porn/)

[6] Palfrey, J., Boyd, D., Sacco, D. and DeBonis, L. (2008) Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States (Harvard University; Berkman Center for Internet and Society). http://www.wiredsafety.org/resources/pdf/2009_isttf_final_report.pdf

[7] Ofcom's UK children's media literacy study published in March 2010 asked participants which of a list of things they didn't like about a social networking site and the responses revealed 24% of 8 – 11 year olds and 25% of 12 – 15 year olds did not like the fact that people could send hurtful messages via social networking sites, in addition to 18% of 8 – 11's and 24% of 12 – 15's recognising that bullying occurs on these sites. http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/ukchildrensml/ukchildrensml1.pdf

[8] www.beatbullying.org/pdfs/Virtual%20Violence%20-%20Protecting%20Children%20from%20Cyberbullying.pdf

[9] See the Australian Covert bullying prevalence study, May 2009, CHPRC, ECU, www.deewr.gov.au/Schooling/NationalSafeSchools/Pages/research.aspx, pxxiii,

[10] This study found that cyberbullying had been experienced by 10% of 10 and 11 year olds, and 16% of 12 and 13 year olds.

sexting happened regularly or 'all of the time'. Additionally, 56% of respondents were aware of instances where images and videos were distributed further than the intended recipient, indicating that the majority of respondents knew that these images and videos were sent on beyond the people for whom they were intended, highlighting where sexting and cyberbullying can converge.[11]

Other risks that children and young people can face include grooming. The UK Sexual Offences Act 2003 defines online grooming as, "a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes."[12] These cases do sadly still occur.

Inappropriate social and health behaviours in an online environment (e.g. technology addiction, online promotion of eating disorders, drug usage, underage drinking, smoking and gambling)

Childnet believes that there are three main risks facing children and young people in the online world. Childnet has defined these risks as content, contact and commercialism, but each of these three areas of risk is underpinned by user conduct. Childnet works with young people to help to shape and influence their behaviour to empower them to be safe online.

Childnet's 5 SMART rules[13] help younger children understand the importance of keeping safe online, and are at the heart of Childnet's education work. One of Childnet's key messages to children and young people as part of the SMART rules is the lesson on reliability.

Reliability - "*Information you find on the internet many not be true, or someone online may be lying about who they are*". This message is shared in various ways with all the audiences that Childnet's Education Team interact with. The messages shared under this topic tackle the risks posed by unreliable information on the internet. Childnet encourages young people to check at least three online sources, to make qualitative judgments about the reputation and validity of a website assessing the authorship of a website and the messages it is trying to promote. This information is important in equipping children and young people to deal with the content based risks that they may be faced with regarding a range of subject areas as suggested in the inquiry's terms of reference.

A lot of the parents that we talk are concerned about over use of the internet and the amount of time that their children and young people spend online. Internet addiction, the spending of excessive amounts of time online at the expense of and to the detriment of other aspects of the user's life is a concern for parents, and Childnet encourages parents to introduce good habits about internet usage with children from the outset, to help them become accustomed to the internet being time-limited and in used in balance with other activities.[14]

Identity theft and breaches of privacy

Social networking has offered users an attractive means of easy, instantaneous means of self-expression. One of the key topics that Childnet covers as part of our outreach work with children is that of privacy. When engaging with the pre-teen audience, particularly younger children aged between 5 and 10, Childnet's privacy messages focus on the importance of keeping personal information, such as full name, email address, phone number, home address, photos, school name and passwords, private. The 2010 Safer Internet Day message of "Think Before You Post" is particularly important for those

[11] www.swgfl.org.uk/Staying-Safe/Sexting-Survey
[12] www.opsi.gov.uk/acts/acts2003/ukpga_20030042_en_1
[13] www.kidsmart.org.uk/beingsmart/
[14] Childnet factsheet on Internet Addiction: www.childnet-int.org/downloads/factsheet_addiction.pdf

who frequently use social media services like Facebook. Information and images online have longevity and an incredible reach, which should be factored into any decision to post content and Childnet encourages all users to think about the possible implications and impact of their posts. We also know of children and young people who have had experiences of unknown others using their photos and in some cases assuming their identity, resulting in them receiving a detrimental credit rating.

Australian and international responses to these cyber-safety threats and opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with these cyber-safety issues

Childnet have been involved with some crucial work in Australia with the ACMA, and we have also worked with the Child Health Promotion Research Centre (CHPRC) at the Edith Cowan University (ECU) in Perth.

ACMA have undertaken a comprehensive and excellent range of work in this area, recently developing and launching the **Cybersmart website**[15] which caters to all audiences, children of all ages, parents and carers, and schools and libraries, and includes quizzes, activities, as well as teaching resources and video.

There are a range of international networks to counter and to deal with the various cyber threats in existence.

In terms of Education and Awareness**, Insafe**[16] is a significant membership organization which coordinates a European network of Awareness Centres promoting safe, responsible use of the Internet and mobile devices to young people. Insafe partners monitor and address emerging trends, while seeking to reinforce the image of the web as a place to learn. They endeavour to raise awareness about reporting harmful or illegal content and services. Through close cooperation between partners and other actors, Insafe aims to raise Internet safety-awareness standards and support the development of information literacy for all. National Safer Internet Centres from across the EU are under the INSAFE umbrella, and organize and run Safer Internet Day in their respective countries. Although it is an EU generated event, it is a Day which is also celebrated worldwide, and ACMA were involved in Safer Internet Day 2010.[17]

The **UK's Home Office Task Force on Child Protection on the Internet** was established in March 2001 in response to concerns about the possible risks to children after a number of serious cases where children had been "groomed" via the internet. In the face of such concerns, the Task Force was a unique collaboration bringing together, in a positive partnership, representatives from the internet industry, children's charities, the main opposition parties, government departments, the police and others who shared the aim of making the United Kingdom the best and safest place in the world for children to use the internet. The work of the HOTF was subsumed in the 2008 creation of the **UK Council for Child Internet Safety** (UKCCIS)[18]. UKCCIS brings together over 140 organisations and individuals to help children and young people stay safe on the internet. It is made up of companies, government departments and agencies, law enforcement, charities, parent groups, academic experts and others.

Of particular note, the Home Office Task Force developed a series of **good practice guidance documents** which set out a series of models of good practice for the provision of different kinds of internet services by a range of companies and organizations active in the online world. These documents were intended primarily as a guide to commercial or other organisations, or individuals, providing online services or considering doing so in the future, but as public documents, are also of

[15] www.cybersmart.gov.au/
[16] www.saferinternet.org/web/guest/about-us#hotlines
[17] www.acma.gov.au/WEB/STANDARD/pc=PC_312038.
[18] www.dcsf.gov.uk/ukccis/

interest to internet users. The guidance covered includes advice on chat, search, moderation and social networking services. ACMA submitted a statement of support for the Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services 2007, as well as participating in the drafting of the guidance. Best practice documents have also been drafted and promoted by industry groups, such as the UK code of practice for the self-regulation of new forms of content on mobiles[19] and the European Commission including Safer Social Networking Principles for the EU[20] and the European Framework on Safer Mobile Use by Younger Teenagers and Children[21].

The UKCCIS Click Clever Click Safe Internet Safety Strategy document launched by the then Prime Minister in December 2009 committed to making sure that a review of how each set of guidance is used would be carried out periodically. These necessary reviews will ensure that parents and young people are confident that the guidance is being applied and understand how. This level of accountability is vital in understanding how the best practice guides are being conformed to and what more needs to be done.

The **Virtual Global Taskforce**[22] was launched in 2003 as an international alliance of law enforcement agencies, bringing together partners from the UK, Australia, the United States of America and Canada as well as Interpol. This association gave the police an online presence and level of cooperation globally. Specifically, membership of the alliance includes the Australian federal police and CEOP in the UK, both of whom have a reporting function.

The **International Telecomm Union**'s (ITU) **Child Online Protection** (COP) **Initiative**[23] aims to tackle cybersecurity holistically, addressing legal, technical, organisational and procedural issues as well as capacity building and international cooperation. The ITU promote a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of an international collaborative network. The key objectives of the initiative are to identify risks and vulnerabilities to children in cyberspace, create awareness, develop practical tools to help minimize risk and to share knowledge and experience.

Teachtoday[24] was launched in 2008 by a unique collaboration of the ICT industry and European Schoolnet, a network of 31 European Ministries of Education, with the support of the European Commissioner for Information Society and Media. It provides information and advice for teachers, head teachers, governors and other members of the school workforce about the positive, responsible and safe use of new technologies.

INHOPE[25] is the International Association of Internet Hotlines. The mission of the INHOPE Association is to support and enhance the performance of Internet Hotlines around the World, ensuring swift action is taken in responding to reports of illegal content making the internet a safer place. The key functions of the Association are exchanging expertise, supporting new hotlines, exchanging reports and providing an interface with relevant initiatives outside the EU. There are thirty six members of INHOPE worldwide, including members from Europe, Asia, North America and Australia. Through meeting regularly to share knowledge and best practice, INHOPE and its members are working to tackle the global problem of illegal content online.

[19] http://www.imcb.org.uk/assets/documents/10000109Codeofpractice.pdf
[20] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf
[21] www.gsmeurope.org/documents/safer_children.pdf?safer_children&ns_type=pdf&ns_url=http://www.gsmeurope.org/documents/safer_children.pdf
[22] www.virtualglobaltaskforce.com/
[23] www.itu.int/osg/csd/cybersecurity/gca/cop/so-whats-cop.html
[24] www.teachtoday.eu
[25] www.inhope.org/

Ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying and the role of parents, families, carers and the community

Childnet has pioneered the **whole-school community** approach in dealing with cyberbullying and this approach has been widely shared with partners globally, including key partners in Australia. Childnet is pleased to have established a relationship with ACMA to support the whole school community in Australia in dealing with incidences of cyberbullying, and to think about establishing programmes of support in and for schools. We have also been involved with the excellent work of Donna Cross and her team at the CHPRC at the ECU.

Childnet helped the UK Department for Children Schools and Families (now the Department for Education) to develop guidance for schools on preventing and responding to cyberbullying. The guidance was designed to help schools recognise what cyberbullying is and to help schools to recognise how it is different from other forms of bullying, outlining the steps schools need to take to help prevent and respond to cyberbullying incidents appropriately. The guidance presented a positive 'Whole-School Community' approach to addressing social problems online, encouraging children, young people and schools to model the constructive use of technology, and to create and engage in safe communities.

Cyberbullying and its potential impact needs to be understood by all members of the school community – children and young people, all teachers (not just the ICT teacher, all school staff, the Head teacher, the governors, the parents and other organizations supporting children. Too often we have heard from young people, '*People don't take cyberbullying seriously because it is not physical*'. Each member of the whole school community has a role to play in preventing and responding to cyberbullying. The important and timely guidance on cyberbullying was localised by ACMA with relevant links and contact details for Australian organisations along with the repurposing of the Lets Fight it Together DVD resource[26] designed to be viewed by pupils, staff and parents, to help build a whole-school community approach to dealing with the problem of cyberbullying. It was launched in Sydney by Chris Chapman, Chair of the ACMA and Will Gardner, Childnet's CEO in September 2009[27]. The Let's Fight it together film has also been repurposed for use in Germany, New Zealand and Denmark.

Childnet also believes that it is important to support the **school staff** who play key roles in shaping, teaching, challenging and supporting young people so that they are fully equipped for the changing culture in which they are operating. It is vital that they are made aware of the types of issues that have been outlined earlier in this response, including cyberbullying, as part of their continuing professional development, and also to be aware of how they can protect themselves and ensure their own safety and security in this environment. In responding to all the potential risks that may negatively impact on children and young people's cyber safety, Childnet believes that school staff should be encouraged not only to address important safety topics with pupils, but should also be provided with a range of easy to use resources to encourage them doing this. For example, Childnet's Know IT All for Primary[28] resource was designed to introduce teachers to key safety issues as well as including an interactive training film to help them understand how to fully use the resource and present the important safety messages as well, as part of their ongoing continuing professional development. This resource has been made accessible to children with Special Educational Needs[29]. It is also being adapted for distribution in Mexico. The Know IT All for Secondary Schools portal[30] provides teachers of secondary aged pupils with a wide variety of ready to use e-safety resources accompanied by downloadable lesson plans, films, games, PowerPoint presentations and more, covering plagiarism, Copyright, Cyberbullying, Grooming, Safer Social Networking and Digital Citizenship. Additionally, Childnet developed the guidance on supporting school staff as potential targets of cyberbullying[31] including tips

[26] www.digizen.org/cyberbullying/film.aspx
[27] www.childnet.com/news/articles/20091021.html
[28] www.childnet.com/kia/primary/
[29] www.childnet.com/kia/sen/
[30] http://childnet.com/kia/secondary/
[31] www.digizen.org/downloads/cyberbullying_teachers.pdf

for staff to help protect themselves. Childnet was delighted to see internet safety included on the UK secondary school curriculum and the 2009 commitment that from September 2011 safe and responsible use of technology would be covered under the primary curriculum.

The **role of parents, families, carers and communities** is also important in responding to potential online risks and in tackling incidences of and the effects of cyberbullying. Childnet believes that there is a shared responsibility to ensure that children understand how to use the amazing and exciting new technologies responsibly online and families, carers and the community undoubtedly have an important role to play here. Listening to the thoughts and concerns of parents in regards to the Internet and the support that they need, "*I know it is helpful for my kids but show me the benefits*" and "*If my child has a problem and I don't know how to help then I'd rather not know!*", Childnet has worked to support 'parental late adopters' of internet technologies to bring them up to speed on the benefits they can receive from the Internet, at the same time as sharing vital information to empower them to help themselves and their children stay safe online. Childnet has achieved this through the award-winning Know IT All for Parents[32] resource. Know IT All for Parents is an interactive and innovative resource available in different formats and languages, designed to empower varied user groups in understanding how the Internet works and how it can be used positively including information on file-sharing, social networking and cyberbullying. Know IT All for Parents has been shared with over 2 million parents in the UK as of June 2010. Reaching parents does present challenges. Following feedback from focus groups ran with parents as part of the development of the resource which revealed that parents trust information coming from schools, the resource was made free for schools to order and distribute to parents. Parents representing ethnic minorities within these focus groups stressed the point that they wanted accessible advice in their own language, and Know IT All for Parents includes a summary of the content in Arabic, Bengali, Gujarati, Mandarin, Polish, Punjabi, Urdu, Welsh and British Sign Language. By working to include a good balance of learning styles such as audio visual presentations and access to written text of the scripts and visual material, Childnet has acted to facilitate the widest possible access to the resource and its key messages, particularly for late adopters of technology, and this is a key audience to reach in helping to promote wide cyber-safety.

As we respond to the issues of staying safe online in 2010, **digital citizenship** is one of the concepts at the heart of Childnet's thinking. At Childnet when we think about digital citizenship, we focus on encouraging the development and growth of safe and secure users of technology, who are able to make informed choices and valuable contributions online that benefit and inspire themselves, other users and the digital community. We believe that digital citizenship is crucial because of the interactive nature of Web 2.0 technologies. Convergence has had a real impact on digital citizenship. For example, users are able to access social networking services via mobile devices. Many mobile devices have cameras on them, so users can instantly upload pictures as they are on the go, and this can be almost instantaneous and so it is very important for digital citizenship to be an embedded part of users thinking so that they internalise it and act on it. The concept of digital citizenship doesn't just apply to children and young people, but to everyone who uses digital technologies and the internet. For example, it is a parent and carers role to be aware of the protections that can be used, such as those that social networking providers have put into place, so that they can help their children/young people to identify a suitable service as well as being aware of what the age limits are on different sites and how a user can limit who accesses their profile to support them in using such services safely.

It is important for all users to think about how to use technology appropriately, and there are considerations of digital citizenship for parents, carers, grandparents and children. In conjunction with Childnet's work on cyberbullying, Childnet launched a unique website called Digizen[33], a composite of the words digital and citizen, exploring this topic and more detail and aiming support and showcase young people's positive social engagement and participation online including an overview of the full guidance document, the film, and other responses to cyberbullying.

[32] http://childnet.com/kia/parents/
[33] www.digizen.org

Conclusions

1. **Children need to be able to make good decisions online, whenever and wherever they are online. It is critical to provide young people with the skills they need to navigate the online environment safely.**

2. **The situation in Australia, just as it is in the UK, is that, whichever research statistic you take, we are seeing that Cyberbullying is a feature of many young people's lives.**

3. **The whole school community approach is vital in achieving cyber-safety and it is imperative to support all those who play key roles in shaping, teaching, challenging and supporting young people, alongside listening to and responding directly to the concerns of children and young people so that they are fully equipped for the changing culture in which they are operating.**

4. **Industry can and must take steps alongside any education initiatives to address and support e-safety, such as engaging in multi-stakeholder dialogue and signing up to best practice guidelines and associated independent monitoring of compliance with guidelines.**

5. **It is key to make sure that all actors in this space – parents, schools, children and young people but also law enforcement, industry and governments are playing their part in making the internet a great and safe place and are supported in this.**

Childnet contacts:

Will Gardner
Chief Executive Officer
will@childnet.com

Lucinda Fell
Policy and Communications Manager
lucinda@childnet.com