Home Office

HOME OFFICE TASK FORCE ON CHILD PROTECTION ON THE INTERNET

Good Practice Guidance for Social Networking and User Interactive Services

December 2006

CONTRIBUTORS

Social Networking and User Interactive Services Project Group

Chair: Annie Mullins – Vodafone (Global Head of Content Standards)
Secretary: Stephen Ruddell – Home Office (Policy Advisor)

Project Team
Graham Anderson – AOL / CEOP
Emma Ascroft – Yahoo! UK & Ireland (Head of Public & Social Policy)
Chris Atkinson – CEOP (Policy Advisor)
Maggie Brennan – CEOP (Research Development and Strategy Advisor)
Jo Bryce – Cyberspace Research Unit (University of Central Lancaster)
John Carr - Children's Charities Coalition on Internet Safety/NCH
Trish Church – Orange (Manager - Community and Abuse Operations)
Julian Coles- BBC Editorial Policy (Senior Editorial Policy Advisor)
Keith Crowell – Piczo. Inc (Director, Member Services)
Camille de Stempel – AOL (Director, Policy)
Cristina Fernandez – National Centre for Missing and Exploited Children (US)
Will Gardner - Childnet International (Research and Policy Manager)
Alex Godger – IWF (Internet Content Analyst)
Liz Harding - MSN, Microsoft Corporation (MSN UK Community Affairs Manager)
Melissa Jordan – Australian Communications & Media Agency (Sr Policy Analyst)
Matt Lambert – MSN, Microsoft Corporation
Professor Sonia Livingstone - London School of Economics
Hamish McLeod – Mobile Broadband Group
Nancy McBride - National Centre for Missing & Exploited Children (US)
Alex Nagle – CEOP (Head of Harm Reduction)
Rachel O'Connell – BEBO (Head of Corporate and Social Responsibility)
Remco Pijpers - (KPN- Holland)
John Shehan – National Centre for Missing and Exploited Children (US)

Other Contributors
Malcolm Hutty – LINX (Head of Public Affairs)
Simon Miller – Department for Education and Skills
Hemanshu Negam - MySpace (Chief Safety Officer)
Matt Nash - Faceparty (Head of Sales & Business Development)

CONTENTS Page

PART 1

PART 2

Good Practice Guidance for Social Networking and User Interactive Services

Introduction

Purpose of Social Networking and other User Interactive Services Generated Good Practice Guidance

Social networking and interactive services offer positive opportunities for children and young people to communicate, interact, share content and interests. This guidance also acknowledges that children and young people may be vulnerable to inappropriate contact via these services and that there is a need to ensure that they are aware of potential risks and empowered to manage their online experience and protect themselves from harm.

This document has been produced to provide advice and guidance to the providers of social networking and user interactive sites. The recommendations provide good practice to promote the safety of children and young people using these services.

The guidance also seeks to:

- Describe the evolution of the Internet and the new social networking and other user interactive services
- Highlight potential risks and safety concerns for children and young people
- Provide good practice recommendations for service providers of social networking and other user interactive services
- Provide advice to users, parents and carers

The Internet and Recent Developments

The World Wide Web has evolved and become an increasingly dynamic and interactive platform in the last two years.

Social networking and user interactive services are now a hugely popular and a compelling activity for many Internet users. These services are considered to be part of a paradigm shift in the evolution of the Internet, which is now frequently referred to as Web 2.0. Simply put, Web 1.0 was characterised by static websites, downloading content, use of search engines, and surfing from one website to the next. Web. 2.0 represents a fundamental shift away from this model, towards a more dynamic and interactive Internet where the creation content is decentralised (not one source) and more controlled by individuals or communities of users.

The convergence of technical and communication platforms is also a significant technological development, for example users can interact with each other across multiple platforms and devices, such as mobile phones, PDAs, game consoles and PCs. This means that users can interact with, post and download content on many different services and on many different devices.

Social networking services – what are they?

Social networking sites allow users to create original content and share it with a vast network of individuals, potentially world-wide. There is now a proliferation of these services, and user generated content is taking a hold in mainstream culture, due to its authentic and original appeal. For example, the number of visitors to MySpace increased from 4.9 million in 2005 to currently over 67 million in 2006

In a very real sense social networking sites are really nothing new. All they have done, albeit rather cleverly, is simply bring together on a single site or to a single place several pre-existing interactive technologies which previously generally had to be accessed separately or independently: chat, search, email, messaging, Blogs, videos and so on. In so doing they may have created a new type of social space but we need to be clear that in terms of the safety aspects they have introduced no new challenges or issues which were not already there, and which had not already been there for several years.

Examples of social networking and other user interactive services

There are a vast number of social networking services worldwide and new services are being launched daily, making it difficult to accurately quantify the sector. *Wikipida*, for example, currently lists over 100 services that operate on global or local basis.

The services vary in terms of audience, features and the range of activities users can engage in. The most common features include:

- Meeting and making new friends i.e. networking
- Posting photos and videos
- Creating and managing Blogs
- Joining member groups with similar interests
- Sharing movies
- Sharing music
- Posting Music reviews
- Sharing thoughts and information on areas of interest
- Playing games

The most popular services currently include My Space, Bebo, Windows Live Spaces, Piczo, Yahoo! 360, Face Party, FaceBook and Xanga. Other services focus on particular features, such as video, but share similar features to social networking services. These include websites such as YouTube, AOL video and Google Video.

Services have also developed around specific communities of interest, which are very popular with children and young people. These services share many of the characteristics of social networking. These include online gaming communities, such as *'Runescape''World of Warcraft, virtual worlds such as 'Second Life', and communities for creating and looking after virtual pets such as 'Neopets'*. Auctioning and trading are also activities children and young people are participating in online, in communities like *'Swapits'*, which has a global currency similar to cash where young people earn rewards, trade and shop. 'All these communities of interest encourage and facilitate social interaction.

Why are social networking services popular with young people?

There are many reasons for the appeal of social networking services. Some of the key attractions include the ability to create original and personal content and publish it in the form of a website, but perhaps most important is the ability for children and young people to express themselves through these services.

Young people enjoy creating their own personal social networking sites, where they can:

- Create and design a personal website using graphics, colour, music and images to install their unique style and identity
- Share music reviews of favourite bands and music that they have composed and performed themselves
- Upload and share images, including pictures of themselves, family and friends.
- Upload and share home made videos they have created
- Create Blogs, journals or diaries about their lives and interests
- Interact with friends in real-time through Instant Messaging, chat rooms or message boards that are integrated into the UG & SN sites
- Receive comments on their personal websites from friends or guests
- Create or join wider communities or groups of interest e.g. football or music
- Link to other friends' personal websites and use RSS to inform friends of any new updates or additions to their websites
- Complete 'ready made' questionnaires integrated into some social networking sites.

Children and the Internet

Being online is part of young people's lives – the evidence base

Sonia Livingstone, Professor of Social Psychology at the London School of Economics and Political Science,[1] has been conducting leading research in the UK concerning children and young people's use of the Internet. The findings of her report, *UK Children Go Online*, give an important insight to children and young people's use of the Internet that are relevant to this guidance[2]. This is important as a context to understanding the risks to children and young people.

Research Findings

- Although children usually consider themselves more expert than their parents, neither children nor parents claim great expertise: 28% of parents and 7% of children (9-19 yrs) who

[1] See http://www.lse.ac.uk/collections/media@lse/whosWho/soniaLivingstone.htm

[2] Following qualitative interviews, observations and focus groups, the main part of this Economic and Social Research Council-funded project consisted of a face-to-face, in-home Computer Assisted Personal interviews with 1,511 9-19 year olds in Spring 2004, plus a written self-completion questionnaire from 906 of the parents of the 9-17 year olds. See www.children-go-online.net for methodology, ethical procedures and all project reports.

use the Internet described themselves as beginners. Low parental expertise is one reason among several why relying on parents to keep their children safe is considered insufficient.

- Up till now, most online contacts have been local rather than distant. For children and young people, the point is to be in constant contact with one's friends and there is little interest in communicating with strangers, although *'friends of friends'* whom one has not met (and whom parents may consider 'strangers') are popular.
- One third of 9 -19 year old daily and weekly users have received unwanted sexual (31%) or nasty comments (33%) online or by text message, though only 7% of parents are aware that their child has received sexual comments and only 4% that their child has been bullied online.
- Also important is the frequency with which children divulge personal information online: 46% say that they have given out personal information to someone that they met online[3]; further, 40% say that they have pretended about themselves online.
- Teens simultaneously know the dangers of contacting new people online but yet still take the risks and actively solicit contact with new people, for example, those who share their interests.
- Teens are both senders and receivers of potentially problematic content. A substantial minority of older teens circulate content they describe as pornography among themselves or those they meet online. Again, more boys than girls do this: 14% of 9-19 year old boys have been sent pornography from someone they know but only 3% of girls.
- Many kids are aware of the risks, but the outcome (from themselves and their parents/teachers) is to increase rules, restrict access, reduce their participation online, and so to reduce the benefits they could gain from the Internet.
- Children and young people may not tell parents about concerns or experiences online for fear of losing their Internet access. Other parental strategies (that seek to reduce risks while not reducing benefits) have not been shown to be effective by research.[4]
- Many young people feel more in control of their actions online than offline. In particular those who have met an online contact in real life, tend to be less shy and they are more likely to be sensation-seekers who are dissatisfied with their lives than those who have not attended a meeting. Like those who make friends online, those who feel more confident communicating online than offline and value the anonymity of the Internet, are more likely to go to meet someone offline.
- Young people value and protect their privacy online, being more concerned about protecting their privacy from their parents than from commercial services[5]. Two thirds (63%) of 12-19 year old home users have taken some action to hide their online activities from their parents, and 69% of 9-17 year old daily and weekly users say they mind their parents restricting or monitoring their Internet use.
- Teens are confident that they can find their way around any system designed to restrict their access online.
- It is socially desirable for children and young people to appear unshockable, making it difficult to determine if children are affected by what they see.

This research predates social networking, but many of the new dimensions of young peoples Internet use are still relevant in this new environment.

[3] Specifically, 9-19 year olds who use the internet at least once per week say they have given out the following information: their hobbies (27%), email address (24%), full name (17%), age (17%), name of their school (9%) phone number (7%) or sent a photograph (7%).

[4] Livingstone, S., Helsper, E., and Bober, M. (manuscript under review, 2006). Balancing opportunities and risks in teenagers' use of the Internet: The role of online skills and family context.

[5] Livingstone, S. (2006) Children's privacy online. In R. Kraut, M. Brynin, and S. Kiesler (Eds.), *Computers, Phones, and the Internet: Domesticating Information Technologies*. New York: Oxford University Press. Pp. 145-167.

It is vital that research continues to update our understanding of children and young people's internet use, particularly as social networking has now become common place.

Using the Internet to test and explore sexuality and identity is commonplace

> *"The Internet is just like life, as I see it, but just easier. So if these 13 or 14 year olds want to find stuff, they're going to find it in real life or on the Internet."* [6]

This quote[7] captures the growing consensus that the activities young people have always engaged in offline they will also do online, and that the convenience, ease and reach of the Internet facilitates these activities, making them more commonplace. [8]

It is a normal part of adolescence to test boundaries, challenge adult norms, experiment with relationships, play with identity, explore new sexual experience, maintain or break secrets, exclude or be excluded by peers, deceive parents and worry about one's development. All this is surely to be expected online as offline. But online, such practices may be spread, manipulated or shared in ways that are easier, quicker, and possibly unexpected in their consequences, compared with offline practices.

As some argue, teens are determined to find out about sex, and to talk about it – but if they can do so anonymously, in a situation of trust, with relatively informed peers, or vicariously by watching television or films about sexual experience – they would prefer this[9].

Other analysis of teenage girls' home pages led to the conclusion that, girls use the Internet not only to express their identity but also to explore – often in a private, intimate, sometimes confessional manner - their confusions, vulnerabilities, uncertainties and ignorance regarding sexuality. [10]

Adolescent social and sexual development and maturity

Views on young people's development are often polarised. In one view, children are seen as vulnerable, undergoing a crucial but fragile process of cognitive and social development to which technology poses a risk by introducing potential harms into the social conditions for development and necessitating, in turn, a protectionist

[6] Lorie, 17, from Essex, interviewed by the *UK Children Go Online* project.

[7] As argued by the recent review by ECPAT International for the United Nations, which brings together a considerable body of evidence regarding the threats to children from cyberspace. As the review points out, cyberspace provides multiple opportunities for adults to harm children, these risks made greater by the ways in which children (and parents) may fail to recognise the consequences of their actions online. See Muir, D. (2005). *Violence against Children in Cyberspace: A Contribution to the United Nations Study on Violence against Children*. Bangkok, Thailand: ECPAT International.

[8] There are problematic gaps in the evidence that mean some will continue to question this consensus (we lack evidence on how young people tested sexual limits before the Internet, for example). Further, many more will question the assumption that the Internet has introduced, or is solely responsible for changing, behaviour (and risks).

[9] Buckingham, D., & Bragg, S. (2004). *Young People, Sex and the Media: The facts of life?* Basingstoke: Palgrave Macmillan.

[10] Stern, S. (2002). Sexual selves on the world wide web: Adolescent girls' home pages as sites for sexual self-expression. In J. Brown, J. Steele & K. Walsh-Childers (Eds.), *Sexual Teens, Sexual Media: Investigating Media's Influence on Adolescent Sexuality* (pp. 265-285). Mahwah, NJ: Lawrence Erlbaum Associates.

regulatory environment. In the contrary view, children are seen as competent and creative agents in their own right whose “media-savvy” skills tend to be underestimated by the adults around them, with the consequence being that society may fail to provide a sufficiently rich environment for them. Clearly, a balance between these two positions would be appropriate.

Cooper, a paediatrician, argues that teenagers’ brains do not reach physical and cognitive maturity until the age of nearly 21 years old.[11] Indeed, most psychologists now consider development to be a lifelong process, with children of different ages showing different degrees and kinds of understanding of personal and social matters as they grow older and as they test themselves against and learn from more complex experiences.[12] The influence of the peer group grows in importance during adolescence as the influence of parents declines (though remains substantial).

What’s ‘normal’ - who is vulnerable?[13]

There is a small body of research that examines the links between internet use and psychological vulnerability. This includes:

- NCMEC’s research indicates that the comparatively small number of psychologically vulnerable children are disproportionately more likely to encounter dangers online and are more likely to suffer harmful consequences.[14].
- An anonymous survey of 50,168 9th-grade (14 -15 year old) pupils, including over 40,000 with home Internet access and 19,511 who accessed chat rooms, was conducted by the US Minnesota Student Survey.[15] This found for both boys and girls, that use of Internet chat rooms was associated with psychological distress, a difficult living environment, and a higher likelihood of risky behaviours. Although most chat room users did not report serious problems, this group included a disproportionate number of troubled individuals. The authors conclude that, chat room use serves as an indicator of heightened vulnerability and risk taking, parents and others need to be aware of potential dangers posed by online contact between strangers and

[11] See http//:www.netsmartz.org/safety/

[12] A fair summary of child development is provided in the table on p.116-7 in Thornburgh, D., & Lin, H. S. (2002). *Youth, Pornography, and the Internet*. Washington, DC: National Academy Press. They describe 13-15 year olds as combining an intense curiosity about sexuality, some sexual activity of varying degrees, being impulsive, and an incomplete skill set in terms of decision-making skills.

[13] See Millwood Hargrave, A., & Livingstone, S. (2006). *Harm and Offence in Media Content: A review of the evidence*. Bristol: Intellect.

[14] Research by the National Center for Missing & Exploited Children based in the US found that those aged 10-17 years old who reported major depressive-like symptoms were 3.5 times more likely to also report an unwanted sexual solicitation online compared to youths with mild/no symptoms. And among those who had been sexually solicited, those who had major depressive symptoms were twice as likely to be emotionally distressed by the incident as those with mild/no symptoms Ybarra, M. L., Leaf, P. J., & Diener-West, M. (2004). Sex differences in youth-reported depressive symptomatology and unwanted Internet sexual solicitation. *Journal of Medical Internet Research, 6*(1),. [14]**.** Note that in this study, it seems likely that depression is both a predictor of unwanted sexual contact and it also exacerbates the distress experienced as a result of such contact e5

[15] Beebe, T. J., Asche, S. E., Harrison, P. A., & Quinlan, K. B. (2004). Heightened vulnerability and increased risk-taking among adolescent chat room users: Results from a statewide school survey. *Journal of Adolescent Health, 35*(2), 116-23.

youth. In other words, it is possible that young people who visit chat rooms may be those more inclined to take risks.

(For full report see **Appendix A**)

Risks to children and young people online

Young people on the whole use the Internet positively but sometimes in ways that may place them at risk of harm. There are a number of potential risks associated with social networking and user interactive services. A young person can be a victim of online abuse e.g. through exposure to harmful content and cyber-bullying. Increasingly young people may also engage in behaviour that is risky to themselves including cyber-flirting and cyber-sex. These situations can quickly escalate to a point where they lose control.

Potential risks to children and young people using social networking services can include but are not limited to:

- Bullying by peers and ‘friends’
- Exposure to inappropriate and/or harmful content
- Sexual grooming, exploitation and abuse through contact with strangers
- Exposure to information about self–harm techniques or encouraging anorexia and suicide
- Racism
- Glorifying activities such as drug taking or excessive drinking
- Encouragement of violent behaviour such as ‘Happy Slapping’[16]
- Physical harm to young people in making video content, such as enacting and imitating stunts and risk taking activities such as playing ‘Chicken’ on railways
- Leaving and running away from home as a result of contacts made online

It is also important to remember that content posted online can impact on a young person’s reputation, both positively and negatively. While social networking services offer great opportunities for children to be creative and express themselves online, children and young people are often not aware that their words or images, although intended for a small audience, can quickly attract a far larger one and have a lasting impact on other people’s perception of them. Some individuals have become notorious resulting in both negative[17] and positive[18] impacts on their lives.

Bullying and Harassment

As an extension of real life, disputes, arguments, gangs and inter-personal tensions also are continued and played out on the Internet. It is therefore no surprise that negative interactions and bullying is by far proving to be the major concern on for children and young people using social networking and user interactive services. Bullying online can manifest in a number of ways social networking and interactive services including:

[16] Happy Slapping is a term which typically describes the filming of violent attacks on mobile phones. Happy Slapping has been called a youth craze which began in school playgrounds in which groups of teenagers slap or mug unsuspecting children or passers-by while capturing the attacks on camera or videophones. http://journalism.bournemouth.ac.uk/lnolan/whatis.html

[17] School kids can be expelled for posting images of bullying conducted during school hours onto social networking sites

[18] The Lulu Blooker Prize is the world's first literary prize devoted to "blooks"—books based on websites such as blogs and webcomics. Blooks are the world's fastest-growing new kind of book and an exciting new stage in the life-cycle of content, if not a whole new category of content. http://www.lulublookerprize.com/

- Posting nasty and negative comments on another users site
- Setting up fake web pages which are attributed to the victim of bullying, which may involve the publishing of doctored pictures and the posting of negative comments on a host of other people's sites.

As well as bullying of young people by young people, some adults, particularly teachers have also found themselves targets of this abuse. This has caused some concern within schools both about the individuals depicted in postings but also the reputation of the school. In some instances these situations have resulted in investigations taking place either by law enforcement or education authorities.

However, in some instances comments posted by students in relation to teachers behaviour, have not been abusive but a form of self-expression about their experiences in school both positive and negative.

These issues highlight the importance of managing bullying and difficult issues within school environments and much work is being undertaken to establish good anti-bullying school policies and the need for schools to have guidance and support to manage children and young people's positive and negative use of the Internet, but specifically 'cyber-bullying' and student dissatisfaction.

It also highlights the need for both parents and teachers to educate and communicate with children young people about the implications of expressing their feelings online and using the Internet to abuse others. In the UK, the Department for Education and Skills newly formed 'Cyber-bullying Task Force' will be developing guidance for schools, parents and children.[19]

Sexual exploitation of children and young people online

It is important to note that by far the most common source of potential harm to children and young people from social networking or user interactive services is online bullying from their peers. There is nonetheless a concern that the capability of the service and children's own high-risk behaviour may present new concerns about the potential for sexual exploitation of children and young people by adults.

This exploitation can include:

- Exposure to harmful content both adult pornography and illegal child abuse images
- Engaging in sexually explicit communications and conversations reducing children and young people inhibitions
- Predators paying young people to pose in sexually provocative ways and pose naked and/or perform sexual acts via webcams
- Grooming and sexual exploitation of children and young people

The 'grooming' process

[19] DfES Cyber bullying Task Force see http://www.dfes.gov.uk/bullying/

Grooming is a process by which a child abuser seeks to prepare a child for later abuse. Abusers use public online interactive spaces to find and meet children and young people. Indeed children and young people can be exploited online without actual physical abuse ever taking place in the real world, for example, by sending and exchanging sexual image paraphernalia, and/or persuading children and young people to send explicit images of them selves. Young people can also be recorded performing sexual acts by child predators through Webcams.

Abusers use a range of techniques to make contact and establish relationships with children and young people including:

- Gathering personal details: age, name; address; cell/mobile number; name of school or a photograph from personal social networking sites, and user generated service profiles
- Offering opportunities for modelling, particularly to young girls
- Promising meetings with pop idols or celebrities; or offers of memorabilia
- Offering cheap tickets to sports or music concerts or events
- Offering material gifts including electronic games, music or software
- Offering virtual gifts (e.g. rewards, passwords, gaming cheats etc…)
- Suggesting quick and easy ways to make money
- Offering and making payment for young people to let view them naked and perform sexual acts via Webcams
- Taking a child in to his/her confidence by encouraging the child to share or talk about any difficulties they may be experiencing, such as bullying or difficult relationships, and offering a sympathetic and supportive response
- Bullying and intimidating behaviour, such as threatening to expose the child by contacting their parents to inform them of their child's communications or postings on a social networking site, and or, telling the young person that they know how to locate them, where they live, or where they go to school
- Using Webcams to spy and take photos and movies of their victims
- Asking sexually themed questions (e.g. do you have a boyfriend? Are you a virgin? Etc…)
- Asking children and young people to meet offline
- Sending sexually themed images to a child (can depict adult content or the abuse of other children)
- Masquerading as a minor or assuming another false identity to deceive a child
- Using schools/hobby sites to gather information about a child's interests, like / dislikes to use as a grooming aid

Having made contact with one young person, abusers may use that young person to contact and get to know their friends. The links to their '*friends'* in interactive services and user profiles can be misused in this way.

The grooming process whatever its guise, can result in many children and young people feeling guilty and responsible for inappropriate interactions, exploitation and/or actual abuse. They can find it extremely difficult to seek help or tell anyone what is happening to them due to their sense of personal responsibility, guilt and shame.

The use of webcams and other technologies to sexually exploit children and young people

In a small number of cases of sexual exploitation of children and young people, hacking technologies such as 'trojans', 'malware' and viruses' have been used to engineer greater control and exploitation over victims. This may include remote access to computers, accessing personal data and controlling webcams.

Young people's use of webcams is a new and growing concern. Webcams raise two main challenges for the safety of young internet users.

First, there are a number of cases where young people have been intimidated into recording explicit images of themselves using webcams and sending them to individuals they meet online. This allows these individuals to build libraries of images and videos of young people who might then be coerced in to further contact by threats that the material may be published or disclosed to their family and friends.

Second, as mentioned above children and young people increasingly use the Internet to explore their sexuality and engage in cyber-flirting or cyber-sex with their online 'friends'. However, they often do not understand the potential implications of sharing or publishing personal images or videos on the Internet. Explicit or suggestive images of a young person can be classified as illegal child abuse or pornography, even if it is posted by the participants.

The risks posed by the technologies highlighted above are not yet well understood and further research is required. Recent research conducted in Holland, involving 10, 900 participants and carried out by the *'My Child Online Foundation'* in 2006, reveals that 47% of girls who responded to the survey, said they had received unwanted requests to do something in front of a webcam – although only 2% actually did so.

It is therefore essential that Internet safety and education programmes address the use of webcams by children and young people, not least because of the permanency and future implications of personal images or videos published on the Internet.

The role of education in keeping children and young people safe online

Education and media literacy is a critical part of keeping children and young people safe online and empowering them to manage their online experience. Responsible use and keeping safe online are now advocated as essential elements of a broad curriculum. In the UK the Child Exploitation and Online Protection Centre (CEOP) has launched a national campaign *'Think U Know'* [20]. This campaign provides young people with advice and guidance on how to have fun, stay in control of their personal information and report any problems they may encounter in the online environment.

Research shows[21] that children and young people receive information about internet safety from a range of sources. Younger children, for example, tend to have rules set for their internet use in the home by their parents and the parental control tools

[20] Think U Know www.thinkuknow.co.uk

[21] See Ofcom's "Media Literacy Audit: Report on media literacy amongst children", http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/children/

are more likely to be installed on the home PC. Parents are, however, less likely to set rules for teenagers. The influence of a young person's peer group therefore becomes more important in influencing their behaviour and attitudes to online services.

It is vital that parents become involved in children and young people's use of the Internet, including social networking and other user interactive services. It is critical that they have direct conversations, particularly with teens on a regular basis about what they are doing online and their experiences.

A key focus for parents in terms of social networking must be, not only what their children are viewing and downloading but what information they are publishing online about themselves and others, including any text, image or video.

It is not the intention of this guidance to provide exhaustive advice or guidance for young people and their parents and carers. There is a wide range of information and advice available both from service providers and from other organisations such as educational bodies and child welfare charities. (See **Appendices B and C** for safety tips for parents, carers and young people).

We would recommend the following key sites for information and advice.

www.thinkuknow.co.uk
www.internetsafetyzone.co.uk
www.getnetwise.org
www.childnet-int.org/blogsafety
www.blogsafety.com
www.nch.org.uk
www.nspcc.org.uk
www.bbc.co.uk/chatguide/
www.netsmartz.org (US)
www.netalert.net.au/ (Australia)
www.wiredsafely.org (US)

Part II

Recommendations for Good Practice for Social Networking and User Interactive Services

The interactive and dynamic nature of social networking services present young people with new opportunities and challenges. These recommendations provide good practice guidance to service providers to support a safer environment for young users.

General principles

- Service providers should consider and act in accordance with previous Home Office Task Force Good Practice Guidance on Chat, Instant Messaging and Web Based Services[22]

- Language and terminology should be accessible, clear and relevant for all users, including children, young people and parents, especially relating to Terms and Conditions, Privacy Policy, key safety information and reporting mechanisms

- These recommendations apply to all platforms. Increasingly service providers are enabling customers to access their account from any platform (i.e. fixed or mobile), so that the facilities are available both at home and on the move. Accordingly the recommendations apply to all services across platforms. Nevertheless, they also allow for practicality and flexibility in implementation to accommodate the different characteristics of each; (for example, the different screen sizes and methods of navigation may call for alternative approaches)

Education by Service Providers

Whilst children and young people will want to make the most of what these services have to offer them they will need to understand the importance of protecting themselves, their online identities and reputations. The provision of education by service providers for users of social networking services is critical.

- Safety information should not only address personal safety issues but also individual responsibilities to respect and protect the wider online community. For example, how to behave responsibly when posting images and comments

- Safety information should be specific to the service being provided, updated to reflect service development, and tested for effectiveness and relevancy for users

- Safety information should include advice on how to use functions or tools which can help protect the user from unwanted contact or communication. For example, 'ignore' functions, removing people from a 'Friends' list or how to review and remove unwanted comments on their Blog or other elements of their site.

[22] See http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ho_model.pdf

- Safety information should include information on how to make a report or complain to the service provider, or elsewhere as appropriate

- Safety messages should be easy to understand. Language and terminology should be accessible, clear and relevant for the target audience e.g. children and young people, parents and carers

- Safety information should be made available during the registration process, prominently available from the relevant home page and in other appropriate places within the service.(e.g. in the welcome email)

- Service providers should offer links to relevant online resources which will provide users with additional information about online safety

- Service providers should also consider providing timely and periodic reminders and updates on relevant safety issues to children and young people

Editorial responsibility

Many providers of social networking services exercise some editorial control over certain content on their site. For example, some providers edit a 'Home Page' where they feature new user profiles or highlight a particularly good site. These recommendations aim to provide guidance on editing such spaces responsibly.

- Service providers should exercise care and judgement in featuring sites created by children and young people

- Providers should be particularly sensitive to the context in which younger users sites are presented and avoid inappropriate juxtaposition. This may include, for example, an under 18 profile appearing next to another with an adult theme or on a page carrying inappropriate advertising

- Advertising displayed on social networking services should be appropriate for the audience. Where a service is aimed at or likely to attract under 18s, providers must follow relevant local guidelines or codes for advertising to minors. In the case of the UK, this is the Advertising Standards Authority code of advertising practice[23]

Registration

Registration is an important first step for authenticating the user and making them aware that they are responsible for their behaviour online. During the registration process, users are asked to provide a certain amount of personal data and agree to the terms of service.

[23] Advertising Standards Authority Code of Advertising http://www.asa.org.uk/asa/codes/cap_code/

- Clear information should be given to the user about what the information required in registration will be used for

- The amount of personal information captured at registration from younger users should be kept to a minimum and comply with legal requirements associated with obtaining informed consent from minors

- Service providers should consider carefully the implications of automatically mapping across personal information disclosed in registration to the user's profile. In this instance users should be informed of this process to afford them the opportunity to protect or change their personal information

- In addition to the Terms of Service, Service providers should consider highlighting, in accessible and easily understood language, *'what behaviour is and is not acceptable on the service'* particularly by young users and for their parents and carers. This serves both to inform the user about the acceptable limits of their own behaviour, as well as frame their expectations of the service from the outset

- Service providers should make it clear to users, that if they contravene the TOS / AUP the provider may take action, including co-operation with law enforcement agencies. By highlighting that users activity is traceable, it may be possible to counteract the common misconception that they are untraceable online and remind them that online actions may have offline consequences

- Service providers should where possible request and validate personal information from users e.g. full name, date of birth and a valid email address. This is important to minimise the risk of impersonation and to enable service providers to protect younger users, enhance accurate identity information and utilise *'backend'* screening and filtering tools for the service

- Service providers should capture an IP address at registration, or MSISDN, if registering from a mobile phone and it should be regularly refreshed with use of the service, e.g. each log in, with a date and time stamp

- Service providers should consider also capturing IP addresses for various online activities to improve traceability for registered and unregistered users (e.g. an unregistered user leaving comments in a user's guest book)

- Service providers should ensure that the default settings are set to private or to the user's approved contact list for those registering as under the age of 18. This means their profile cannot be viewed or contacted except by 'friends' on their contact list unless they actively choose to change their settings to public or equivalent

- In services that are pre-moderated where all information is reviewed for full publication by a trained moderator it may be appropriate to set defaults as public. This particularly applies where personal information in profiles is very limited i.e. data fields limited to only nickname, general location, age and personal interests

- Careful consideration should be given by service providers of features, which allow the automatic integration of one or more existing contact lists or address books in to a user's 'Friends' list. Integration of these lists should require prior consent of the user and remain under user control

Creating a profile and user controls

A profile is an easy to create web-page where users can post personal information about themselves including name, email address, telephone numbers, images and videos, of themselves, friends and family, as well as stating interests and hobbies.

- Service providers should ensure that users are aware what information they put in their profile will be made public or private, and understand what this means. In particular users should be made aware of the available options regarding searchability of their profile or webpage

- Users should be made aware when opting to become public their profile or web page may become searchable both on the site and via search engines

- Service providers should consider giving users an option to be public on the site but not searchable via search engines

- The status of the profile should be clear to the creator of the profile at all times e.g. is it public or is it private

- Advice should be given to users when creating their profile about the implications of posting information both from a safety and responsible use perspective. For example, the implications of posting a personal photo that contains location information, the risk of using inappropriate user names and images and of posting photos of other people without their permission

- Service providers should consider reminding users when up-loading photos of the terms of service and/or acceptable use conditions, e.g. "*Photos may not contain nudity, violent or offensive material, or copyrighted images. If you violate these terms, your account will be deleted"*

- Service providers should be careful not to encourage under18s to disclose excessive personal data in their profile

- Service providers should also make it clear what options users have to adjust privacy settings and to manage *'who sees what' and* who they interact with. For example, these settings could include features which allow users to select who can leave Blog comments or post content on their pages

- These adjustable privacy settings should be applicable to all aspects of the service for such things as journals Blog entries, image galleries, guest books etc

- Where communications tools such as email, chat and instant messenger are integrated in to a service, the online presence should match the selected privacy setting e.g. if profile is set to private, only identified friends / buddies should be able to view the online presence/ availability

- Service providers should attempt to screen or review user profile photos for under 18s using human and/ or technical moderation, to remove inappropriate content posted by users, but particularly sexually provocative images and videos

- Service providers should consider enabling users to report profiles that may be inappropriate and / or placing a child or young person at risk e.g. report abuse mechanisms

Search

Search applications can be powerful tools finding users of social networking services. It is important that service providers consider the risks associated with providing such tools to identify users who are under 18.

- Service providers should take steps to ensure that private profiles of under 18s are not searchable, either on the service or via search engines (i.e. not indexing profiles for algorithmic search)

- Social networking services with an integrated site search facility should not allow users to search **public profiles** of under 18s using sensitive data fields e.g. age, sex and location

Abuse Management

Service providers employ various approaches to limit the ability of users to abuse a service or harass and annoy other users, as well as post content which breaches the terms and conditions of the service in other ways. As mentioned above, services often have features to empower users to protect their online experience - e.g. allow users to remove or ignore individuals on their ‘Friends’ list or select individuals who can leave comments on their Blog. Some providers moderate services and others provide technical solutions to protect users on their service, or a combination of both. Many technologies are still in early stages of development and, like any new technology, they are not a panacea for the safety challenges social networking services present. Nevertheless, some service providers have deployed these approaches and they have shown promise in detecting and preventing breaches in their terms of use to the benefit of young users and adults alike.

Content screening and moderation

Content review processes can be helpful in detecting user content which may be inappropriate for a younger audience.

- Service providers should employ effective ways of screening under 18 profile photos either before going live on a site or within a reasonable time afterwards

- Where moderators are used practices should follow the Home Office Good Practice Guidance for Moderation of Interactive Services for Children[24].

Adult and age inappropriate content

- Service providers should introduce tools to minimise the risk of users under the age of 18 years browsing and accessing a range of adult and other age inappropriate content.

- Fore example service providers may allow users to tag or label content as being 'adult' in nature or otherwise age inappropriate. A service provider may reserve the right to label or tag users content or to offer technical means of protection.

- Service providers should inform users about what is and is not appropriate content to post.

- Social networking providers who have specific services aimed at adults (e.g. sexual content, and dating or flirting sites) should ensure that these areas are not accessible to users registered under 18 years.

- Providers should also consider using available age verification systems to verify that users accessing adult content or services are over 18 years (e.g. by credit card check, PIN protections or proof of account ownership).

REPORTING CONCERNS, ABUSE AND ILLEGAL BEHAVIOUR

Background

Increasingly, Service Providers are extending the scope of the Customer Care and Report Abuse options available to users to include links to external agencies, including, e.g. confidential helplines, law enforcement support and information lines.

Service Providers therefore need to provide clear and concise information with respect to the options they make available to users to report abuse or difficulties.

[24] See http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/moderation-document-final.pdf

Service Providers and law enforcement agencies have a proven track record in cooperating effectively to combat illegal activities online using well established protocols and procedures. This needs to be extended with the emergence of new agencies, such as the Child Exploitation and Online Protection Centre **(Appendix D)**. In particular, both existing and emerging online law enforcement agencies are tasked with handling reports pertaining to illegal content and activities in a timely manner.

Introduction

It is important for users of social networking and user interactive services, and particularly users under 18, to have clear and easy-to-use mechanisms to report content and behaviour that cause them concern to service providers, public agencies or law enforcement. Service providers should also have appropriate arrangements in place to liaise directly with law enforcement agencies about reports, which may lead to a criminal investigation.

Users of social networking services need suitable mechanisms to report a variety of illegal, other inappropriate communications or other behaviours which breach the providers' terms and conditions. These could include[25]:

- Child abuse images
- Suspicious behaviour towards children & young people, including grooming
- Bullying / Harassment
- Posting of inappropriate content e.g. information promoting or encouraging self-harm and suicide
- Incorrectly tagged adult or age-inappropriate content
- Other forms of criminal behaviour

General recommendations

- Service providers should have in place effective reporting mechanisms for users to report any concerns or abuse to them. Effective abuse management mechanisms should be place in order to respond and manage any user reports

- Service providers should also ensure they have effective links to other external agencies to report the range of concerns and abuse that can be experienced online

- Service Providers should place links to reporting options and advice in prominent positions on relevant parts of their service e.g. where users are interacting with other users, such as in instant messenger, chat areas, picture galleries, user profiles, message boards, guest book areas and Blogs

[25] This list is not intended to be exhaustive. Reporting mechanisms can also be used to report other types of abuse such as copyright infringements, suspected fraud and spam/viruses.

- Providers should consider establishing a general page with links where users can choose the appropriate agency or organisation to whom they wish to report. This could include the service provider, law enforcement, child welfare organisations, other agencies e.g. Samaritans, Internet Watch Foundation, NSPCC, ChildLine and Crimestoppers

- Some victims of abuse or those with concerns may be reluctant to identify themselves or report directly to the service provider or law enforcement. Service providers should direct users to sources of expert help and advice (both online and offline) by providing links to relevant organisations such as child welfare charities and confidential help lines or support services

- Reporting mechanisms should automatically capture (or encourage users to save and send) essential information and relevant evidence - e.g. a 'screen grab' of abusive, offensive or inappropriate content, the online ID of the user and abuser and the date and time of the incident being reported[26]

- Service providers should advise customers to contact the emergency services where there is an immediate threat to safety of life or children are at *immediate* risk of harm, i.e. phone 999 (UK), 112 (Europe) or 911(US)

- Service providers should establish reporting mechanisms that ensure minimal delay in the referral of reports of serious abuse or concerns to the appropriate agency

- The language on websites used to describe how to report abusive, offensive or inappropriate content should be accessible and easily understood by children and young people. Clear messages help to minimise barriers to reporting, and reassure children and young people that reports will be treated seriously

Report acknowledgements

- All reports of abuse should receive an acknowledgment that the report has been received and will be managed appropriately

Public reporting to relevant authorities

- It is important to have reporting links and options for users to enable them to report incidents which are most appropriately sent direct to a specific authority rather than the service provider. This should include, for example, reporting suspected incidents of sexual exploitation of children to CEOP and reporting child abuse images to the Internet Watch Foundation or concerns to the relevant advice agencies

[26] See previous Home Office Task Force guidance on chat and instant messaging.

- Service providers should include relevant information on, and links to, these reporting links or options on their customer care pages. Providers could also provide this information in other ways, e.g. in automated email 'responders' to customers reporting abuse

Reporting arrangements between service providers and law enforcement and child protection agencies

- Providers should agree arrangements with their local law enforcement point of contact to share user reports about potentially illegal behaviour relating to the protection of children e.g. CEOP in the UK. These arrangements should include agreed guidelines on what information service providers should preserve, circumstances under which it is appropriate to share specific private customer data with law enforcement and protocols for their disclosure, which are compliant with the Data Protection Act and other relevant legislation

APPENDIX A

Children and the Internet – Sonia Livingstone (Professor of Social Psychology LSE)

Being online is part of young people's lives – the evidence base

Data on young people's internet use changes rapidly. In the UK, nearly all teens use the internet and mobile phones, many of them extensively. As use of the internet increases, use of television decreases.

What changes a little more slowly is the way in which young people use, and think about, the internet. Relevant to the activities associated with social networking, the UKCGO study[27] found that:

- Although children usually consider themselves more expert than their parents, neither children nor parents claim great expertise: 28% of parents and 7% of children (9-19 yrs) who use the Internet described themselves as beginners. Low parental expertise is one reason among several why relying on parents to keep their children safe is considered insufficient.
- Most online contacts are local rather than distant. For children and young people, the point is to be in constant contact with one's friends and there is little interest in communicating with strangers, although *'friends of friends'* whom one has not met (and whom parents may consider 'strangers') are popular.
- One third of 9 -19 year olds daily and weekly users have received unwanted sexual (31%) or nasty comments (33%) online or by text message, though only 7% of parents are aware that their child has received sexual comments and only 4% that their child has been bullied online.
- Also important is the frequency with which children divulge personal information online: 46% say that they have given out personal information to someone that they met online; further, 40% say that they have pretended about themselves online.
- Teens simultaneously know the dangers of contacting new people online but yet still take the risks and actively solicit contact with new people, for example those who share their interests.
- Teens are both senders and receivers of potentially problematic content. A substantial minority of older teens circulate pornography among themselves or those they meet online. Again, more boys than girls do this: 14% of 9-19 year old boys have been sent pornography from someone they know but only 3% of girls.[28]
- Nearly half (46%) of children and young people say that they have given out personal information, such as their hobbies (27%), email address (24%), full name (17%), age (17%), name of their school (9%) phone number (7%) or sent a photograph (7%), to someone that they met on the Internet.
- Many kids are aware of the risks, but the outcome (from themselves and their parents/teachers) is to increase rules, restrict access, reduce their participation online, and so to reduce the benefits they could gain from the Internet. Other parental strategies (that seek

[27] See www.children-go-online.net

[28] Research by Bocij suggests also that there is a growing phenomenon of online harassment or 'cyberstalking', which Bocij argues is qualitatively different from offline stalking. Among a sample of 235 US undergraduates, nearly 1 in 3 reported some form of 'unwanted pursuit' on the Internet. Young people are not always able to cope with these, including the minority who experienced more severe forms of online harassment or pursuit. Research also finds a modest link also between online and offline stalking, leading the authors to call for greater awareness of the range of available coping strategies as people face online threats from other members of the public. See Bocij, P., & McFarlane, L. (2003). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal, 139*, 31-38. See also Millwood Hargrave, A., & Livingstone, S. (2006). *Harm and Offence in Media Content: A review of the evidence*. Bristol: Intellect.

to reduce risks while not reducing benefits) have not been shown to be effective by research.[29]

- Children and young people may not tell parents about concerns or experiences online for fear of losing their Internet access. Other parent strategies (that seek to reduce risks, while not reducing benefits) have not been shown to be effective by research[30].
- Many young people feel more in control of their actions online than offline. In particular, those who have met an online contact in real life, tend to be less shy and they are more likely to be sensation seekers who are dissatisfied with their lives than those who have not attended a meeting. Like those who make friends online, those who feel more confident communicating online than offline and value the anonymity on the Internet, are more likely to go to meet someone offline.
- Young people value and protect their privacy online, being more concerned about protecting their privacy from their parents than from commercial services[31].. Two thirds (63%) of 12-19 year old home users have taken some action to hide their online activities from their parents, and 69% of 9-17 year old daily and weekly users say they mind their parents restricting or monitoring their Internet use.
- Teens are confident that they can find their way around any system designed to restrict their access online
- It is socially desirable to appear unshockable, making it difficult to determine if children are affected by they see.

This research predates social networking, but many of the new dimensions of young people s Internet use are still relevant in this new environment.

It is vital that research continues to update our understanding of children and young peoples' Internet use, particularly now social working has become common place.

.

Using the Internet to test and explore sexuality and identity is commonplace

> *"The Internet is just like life, as I see it, but just easier. So if these 13 or 14 year olds want to find stuff, they're going to find it in real life or on the Internet."* [32]

This quote captures the growing consensus that the activities young people have always engaged in offline they will also do online, and that the convenience, ease and reach of the Internet facilitates these activities, making them more commonplace.[33] There are problematic gaps in the evidence that mean some will

[29] Livingstone, S., Helsper, E., and Bober, M. (manuscript under review, 2006). Balancing opportunities and risks in teenagers' use of the Internet: The role of online skills and family context.

[30] Livingstone, S., Helsper, E., and Bober, M. (manuscript under review, 2006). Balancing opportunities and risks in teenagers' use of the Internet: The role of online skills and family context.

[31] [31] Livingstone, S. (2006) Children's privacy online. In R. Kraut, M. Brynin, and S. Kiesler (Eds.), *Computers, Phones, and the Internet: Domesticating Information Technologies*. New York: Oxford University Press. Pp. 145-167.

[32] Lorie, 17, from Essex, interviewed by the *UK Children Go Online* project.

[33] As argued by the recent review by ECPAT International for the United Nations, which brings together a considerable body of evidence regarding the threats to children from cyberspace. As the review points out, cyberspace provides multiple opportunities for adults to harm children, these risks made greater by the ways in which children (and parents) may fail to recognise the consequences of their actions online. See Muir, D. (2005). *Violence against Children in Cyberspace: A contribution to the United Nations Study on Violence against Children*. Bangkok, Thailand: ECPAT International.

continue to question this consensus (we lack evidence on how young people tested sexual limits before the Internet, for example). Further, many more will question the assumption that the Internet has introduced, or is solely responsible for changing, behaviour (and risks).

These qualifications aside, the consensus seems reasonable. Since it is a normal part of adolescence to test boundaries, challenge adult norms, experiment with relationships, play with identity, explore new sexual experience, maintain or break secrets, exclude or be excluded by peers, deceive parents and worry about one's development, all this is surely to be expected online as offline. But online, such practices may be amplified, spread, manipulated or shared in ways that are easier and quicker than offline, and also unexpected in their consequences because of the socio-technological infrastructure of the Internet.

Brown[34] argues that those particularly in need of sexual information – her focus is on early maturing girls – are more likely to turn to teen media such as music, magazines and the Internet in search of positive and helpful information about sexuality (precisely because their immediate peers are not yet ready to engage with such issues) but that what they find is that there are relatively few positive depictions of sexuality across most media, compared with negative or problematic depictions. Buckingham and Bragg also argue that the plethora of negative images of sexuality is problematic partly because of the relative absence of positive images.[35]

The authors contributing to Mazzarella's volume, 'Girl Wide Web',[36] are clear that teenage girls need, and will actively seek out, opportunities to discuss sexuality among their peers. Grisso and Weiss comment (p.31), 'Communicating in their own words helps girls develop not only their sense of self and identity but also allows them to construct their own social reality as members of peer groups'. They continue, *'girls will be most free to explore and construct their identities and express feelings about the issues of greatest importance to them when they are in a space they consider safe – that is, free from the potentially judgmental or inhibiting influence of adults or male peers'* (p.32). Analysing contributions to an American site called gurl.com, they discuss as part of normal and healthy sexual development, teens discussions of oral sex, pregnancy risks, sexual positions, emotions associated with sex, their body/genitals, same-sex attraction, etc.

As Buckingham and Bragg argue, teens are determined to find out about sex, and to talk about it – but if they can do so anonymously, in a situation of trust, with relatively informed peers, or vicariously by watching television or films about sexual experience – they would prefer this. They comment (p.61): *'Learning about sex and relationships thus appeared to be seen as a form of bricolage, a matter of 'piecing it together' from a range of potential sources. It was also often a collective process, conducted among the peer group'*.

[34] Brown, J. D., Halpern, C. T., & L'Engle, K. L. (2005). Mass media as a sexual super peer for early maturing girls. *Journal of Adolescent Health, 36*(5), 420–427.

[35] Buckingham, D., & Bragg, S. (2004). *Young People, Sex and the Media: The facts of life?* Basingstoke: Palgrave Macmillan. What is meant by negative depictions? Arguably, depictions of sexuality that are 'out of context', that emphasise a narrow and restrictive conception of (usually female) attractiveness, that are associated with hostility or violence, etc.

[36] Mazzarella, S. R. (Ed.). (2005). *Girl Wide Web: Girls, the Internet, and the negotiation of identity*. New York: Peter Lang.

Stern's[37] analysis of teenage girls' home pages led her to conclude that, girls use the Internet not only to express their identity but also to explore – often in a private, intimate, sometimes confessional manner - their confusions, vulnerabilities, uncertainties and ignorance regarding sexuality.

Adolescent social and sexual development and maturity

Views on young people's development are often polarised. In one view, children are seen as vulnerable, undergoing a crucial but fragile process of cognitive and social development to which technology poses a risk by introducing potential harms into the social conditions for development and necessitating, in turn, a protectionist regulatory environment. In the contrary view, children are seen as competent and creative agents in their own right whose "media-savvy" skills tend to be underestimated by the adults around them, with the consequence being that society may fail to provide a sufficiently rich environment for them. Clearly, a balance between these two positions would be appropriate.

Cooper, a paediatrician, argues that teenagers' brains do not reach physical and cognitive maturity until the age of nearly 21 years old.[38], but most psychologists now consider development to be a lifelong process, with children of different ages showing different degrees and kinds of understanding of personal and social matters as they grow older and as they test themselves against and learn from more complex experiences.[39] The influence of the peer group grows in importance during adolescence as the influence of parents declines (though remains substantial).

Coleman and Hendry[40] argue that sexual experimentation among adolescents represents a growing historical trend (as measured, for example, in trends in age of first intercourse), partly because society has become increasingly open in its representation of sex, including through the media. They cite a considerable amount of research showing that children with divorced or separated parents become sexually active earlier, that parental and peer discussion and attitudes influence teens strongly, and that girls' sexual activity is particularly influenced by social factors (i.e. attitudes and activities of others).

They also add, on the task of parental mediation, *'Where parents see themselves as losing control over the young person's behaviour they are likely to do one of two things. They may become more anxious, and resort to an increasing use of coercive discipline… Alternatively, adults who have low perceived control may become depressed and develop a sense of helplessness about their role as parents'* (p.92-3).

[37] Stern, S. (2002). Sexual selves on the world wide web: Adolescent girls' home pages as sites for sexual self-expression. In J. Brown, J. Steele & K. Walsh-Childers (Eds.), *Sexual Teens, Sexual Media: Investigating Media's Influence on Adolescent Sexuality* (pp. 265-285). Mahwah, NJ: Lawrence Erlbaum Associates.

[38] See http//:www.netsmartz.org/safety/

[39] A fair summary of child development is provided in the table on p.116-7 in Thornburgh, D., & Lin, H. S. (2002). *Youth, Pornography, and the Internet*. Washington, DC: National Academy Press. They describe 13-15 year olds as combining an intense curiosity about sexuality, some sexual activity of varying degrees, being impulsive, and an incomplete skill set in terms of decision-making skills.

[40] Coleman, J., & Hendry, L. (1999). *The Nature of Adolescence* (Third ed.). London: Routledge.

What's normal, who is vulnerable?[41]

The National Center for Missing & Exploited Children (aged10-17 years old) found that those who reported major depressive-like symptoms were 3.5 times more likely to also report an unwanted sexual solicitation online compared to youths with mild/no symptoms, and among youths reporting an Internet solicitation, youths with major depressive-like symptoms were twice as likely to report feeling emotionally distressed by the incident compared to youths with mild/no symptoms[42]. Note that in this study, it seems likely that depression is both a predictor of unwanted sexual contact and it also exacerbates the distress experienced as a result of such contact.

Further, from the overall sample, 19% were involved in online aggression: 3% were aggressor/targets, 4% reported being targets only, and 12% reported being online aggressors only. Youth aggressor/ targets reported characteristics similar to conventional bully/victim youth, including many commonalities with aggressor-only youth, and significant psychosocial challenge. The researchers concluded that youth aggressors and targets (victims) are intense users of the Internet who view themselves as capable web users. Beyond this, however, these young victims report significant psychosocial challenges, including depressive symptoms, problem behaviour, and traditional bullying. The aggressors also faced multiple psychosocial difficulties, including poor relationships with their parents, substance use and delinquency.[43]

An anonymous survey of 50,168 9th-grade (14 year old) public school students, including over 40,000 with home Internet access and 19,511 who accessed chat rooms, was conducted by the Minnesota Student Survey.[44] This found for both boys and girls, that use of Internet chat rooms was associated with psychological distress, a difficult living environment, and a higher likelihood of risky behaviours. Although most chat room users did not report serious problems, this group included a disproportionate number of troubled individuals. The authors conclude that, chat room use serves as an indicator of heightened vulnerability and risk-taking, parents and others need to be aware of potential dangers posed by online contact between strangers and youth. In other words, it is possible that young people who visit chat rooms may be those more inclined to take risks; more research is, once again, needed to understand risk-taking among teens in relation to the Internet and other new media.

Taking another approach to vulnerability, an analysis of reported suicide attempts among young people found that sexual orientation, behaviour and identity did not predict suicidal attempt status, but suicide attempters experienced higher levels of both generic life stressors (low self-esteem, substance use, victimization) and gay-related stressors, particularly those directly related to visible (femininity) and

[41] See Millwood Hargrave, A., & Livingstone, S. (2006). *Harm and Offence in Media Content: A review of the evidence*. Bristol: Intellect.

[42] Ybarra, M. L., Leaf, P. J., & ener-West, M. (2004). Sex differences in youth-reported depressive symptomatology and unwanted Internet sexual solicitation. *Journal of Medical Internet Research, 6*(1).

[43] Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: a comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry, 45*(7), 1308. Ybarra, M. L., & Mitchell, K. J. (2004). Youth engaging in online harassment: Associations with caregiver-child relationships, Internet use, and personal characteristics. *Journal of Adolescence, 27*, 319-336.

[44] Beebe, T. J., Asche, S. E., Harrison, P. A., & Quinlan, K. B. (2004). Heightened vulnerability and increased risk-taking among adolescent chat room users: Results from a statewide school survey. *Journal of Adolescent Health, 35*(2), 116.

behavioural (gay sex) aspects of their sexual identity. Although those who participated in an online support-group attendance were more likely to make suicide attempts, they also had greater life stressors, making the direction of causality difficult to establish.[45]

Sonia Livingstone, December 2006

[45] Savin-Williams, R. C., & Ream, G. L. (2003). Suicide attempts among sexual-minority male youth. *Journal of Clinical Child and Adolescent Psychology, 32*(4), 509.

APPENDIX B

SAFETY TIPS FOR PARENTS AND CARERS

The following sections outline the safety messages for parents, carers, children and young people. These tips draw on the available research, discussed above, and issues discussed in the Home Office project group. The information below is not an exhaustive list and are intended to inform any awareness work in this area.

Safety Tips for Parents on Social Networking and User Interactive sites

1. **Become familiar with social networking and user interactive sites**
   - Parents and carers should become familiar with the social networking and user interactive sites their children are using.

   - Ask your child what social networking and user interactive sites they use and how they work. This will help you understand your child's habits and enable you to assess how well they understand the issues associated with using the service

   - Visit the sites and familiarise yourself with the services the sites have on offer, such as creating a web-space, creating a profile, blogging, making friends etc…

   - Negotiate with your child to visit and view their personal social networking site, if they have one

   - If you are concerned about a social networking web-space your child has created, some service providers will allow a parent or guardian to remove their child's account and space

2. **Striking a balance**
   - Children and young people have strong views about their privacy and it will be important for you to help your child to use social networking sites responsibly and safely

   - There is an important balance between educating children and young people about the risks online, viewing what they are doing and actually trusting them in their use of social networking sites, and allowing them a degree of autonomy

3. **Guarding privacy**
   - It is critical that children and young people understand the importance of protecting their privacy online. Many, if not all of the key Social Networking sites provide privacy tools to ensure users can manage who they choose to interact with and the *'friends'* that can place comments on their blogs or personal sites

- It is important that children and young people think carefully about adding a stranger to their *'friends list'* even if another friend has recommended them – people are not always who they claim to be

- Talk to your child about the importance of keeping the password to their Social Networking account or space private to protect against someone taking control of their site or space

- Ensure that your child is aware of the privacy setting options of their account. It is important that you negotiate with your child the appropriate level of privacy and that it matches their level of emotional maturity and understanding

- Advise your child of the potential risks in sharing any information that may help locate them in the real world, for example, whether any images have a precise place name

4. Managing personal images and video postings

The use and sharing of images and videos has exploded online especially on social networking and video sharing sites.

- It is very important that children and young people consider and choose carefully what they share online with friends and the wider community on the Internet, especially as photos can be easily copied and changed

- Photos can contain information, which, on its own may seem innocuous, but when put together with other information (e.g. school details) can be used to locate and identify the child

- Photos should be suitable i.e. not provocative, so as not to attract unwanted attention from adults who may wish to exploit children and young people

- Check the 'Acceptable Use' policies of Social Networking and other interactive sites. Most sites will remove explicit and 'inappropriate' images when they are brought to their attention

- Check with your child whether they are comfortable with the content they are posting being seen by everyone they know and whether it might embarrass them at a later stage

5. Managing comments and postings

Many youngsters go to great lengths building their web-spaces, so receiving comments from the wider community can be exciting, compelling and is expected.

- It is important that children and young people understand the need to be responsible in what they post and contribute to other people's social networking sites – *'think before you post'* is a good maxim

- There have been some incidents of bullying often amongst known friends on Social Networking sites – whereby bullying in the playground has continued and possibly escalated online. The potential to humiliate and harass individuals through comments and posting images can be extremely hurtful and have a number of unintended consequences, such as spreading very quickly to a much larger audience online. It is important for parents to set rules with their children about what is OK and what is not OK to post about anyone known or unknown

- Emphasise to your child that once a comment or a posting is made it may not be possible to retract it

6. Managing your kid's flirtatious behaviour

- It is important that parents discuss and establish boundaries about flirting online with your child from an early age e.g. when your child begins to show an interest in and is beginning to use interactive services

- Teens may engage in flirting or sexual exploration online and it is important to discuss the need for boundaries in relationships even with known boyfriends and girlfriends

- Parents and guardians should discuss, and emphasise, particularly with older teens, the dangers of flirting with strangers online. As some people lie about who they really are, no one really knows who they are interacting with.

7. Meeting up with online *'friends'* or strangers

Meeting *'online friends'* in the real world is not new or particular to social networking or user interactive sites. Children and young people often assume that those people they have spent time interacting with online are real friends and therefore safe to meet. However, as with all meetings with strangers there may be risks and great caution should be applied.

- It is important for children and young people to think very carefully before agreeing to meet anyone they have met online and agree any such meetings with their parents or carers

- Parents should ensure that any meetings with '*online friends'* takes place in public and with trusted friends or adults present

- It is important for parents to address and monitor the possibility of their children's involvement in being involved in organised 'gang' meetings in the real world, which are arranged online for fights and other nefarious activities. This is currently emerging as an issue in certain communities, for example sectarian, racist and religious hatred

8. Getting help and reporting abuse

- It is critical for parents and carers to maintain an ongoing dialogue and have regular conversations with their children about anything that is worrying them or has happened online

- If you suspect that your child or another child is being solicited online or is being *'groomed'* by someone with a sexual interest in children it is important to report it to the appropriate authorities

- If you have any copies of communications, images, messages or other content related to the solicitation of a children it is important to keep them and pass to law enforcement

- It is very important that both you and your child understands how to report anything that might be inappropriate or illegal either to the service provider, law enforcement or other designated agency

- There are now a number of places to report potential illegal behaviour online, for example, in the UK the Child Exploitation and Online Protection (CEOP) (www.ceop.org.uk), in the US the NCMEC Cybertipline (www.cybertipline.com)

APPENDIX C

SAFETY TIPS FOR CHILDREN AND YOUNG PEOPLE

Many children and young people have a web-space or belong to an online community. These are lots of fun, and can be a great place to share your interests, - communicate with friends and learn new skills in using technologies. However, as in the real world, it is important that you take care of yourself, your friends and the wider community.

Keep Control
Social networks and interactive services are used primarily to connect with friends you know in the real world. Therefore, you might not immediately consider the need to be cautious about the information you put on your web-space. However, connecting with *'friends of friends'* and even *'friends of friends of friends' may* mean that you are providing information to the sorts of people you would not necessarily be so open with in the real world. Therefore you should consider the following;

- Before setting up your web space think about who it is you want to connect to and who else will be able to view your web-space?
- If you want to limit access to your web space to your real world friends and family, you need to set your Privacy settings to *'Private'* or '*Buddy/ friends'* list'
- Check that the Settings or Preferences of the particular service you are thinking about using allow you to operate in a p*rivate mode'*
- 'Private mode' may be safer than *'public mode'* but remember, disputes can still occur between the closest of friends and your content may be misused e.g. to bully you or to damage your reputation. Therefore, think very carefully about what you share with your friends
- You must protect your password to your web-space and not share it, even with your friends to limit the risk of others gaining control of your web-space

'Going Public'
If you intend to 'go public' to communicate and share your content such as video clips, images and music you've created with the whole social networking community, it is important to think about the following:

- Be cautious. 'Going public' may have unintended consequences!! It is a good idea to be far more careful about the kind of information you share about yourself and how you manage your online reputation
- Remember, when you 'go public', it is not just *'friends of friends of friends'* but actually anyone can view your content, search and find you online

‘Loading up’

Some of the best things about social networking include the ability to ‘load up’ your content online, for example, images, videos and music that you have created and to experience other people’s reactions to it. It is also very exciting to access and comment on others people’s content. However, there are some basic things you should consider before ‘loading up’.

- Is the content appropriate for the intended audience and how might it be used or misused by others? For example, pictures can be copied and altered and posted elsewhere

- Information you post will also reflect the kind of person you are, and will influence how others perceive you

- Guard your online reputation. Think carefully before uploading content and sharing information on your profile or blog that shows you or your friends in any compromising situations. Seek permission from your friends before you ‘load up’ content. Protect your friends and family, they have reputations too!

- Remember what may seem funny to you actually can be very hurtful and offensive to others – so ‘think before you post comments on other people’s web-spaces

- Do not post content that could be viewed as racist, homophobic, bullying, or threatening. Remember these sorts of behaviours could result in your web-space account being closed by the service provider, and the possibility of law enforcement becoming involved

- You need to take care before uploading any images of you posing in a sexually provocative way. Unfortunately, there are people on the Internet who may misuse these images in ways that could cause you a lot of upset

- Try not to bring disputes, arguments and hostilities toward others that you know in real life into the online community

- Setting up a fake web-space to pose as someone else may seem like an effective way to cause embarrassment to the person you are impersonating. However, this type of activity can have very serious consequences, not only in terms of the distress and hurt you may cause to another person but it may also lead to intervention by law enforcement agents

- It important that you understand that **you are not anonymous online** and can be traced even if you provide a fake email account and registration information. Every computer and device connected to the Internet is allocated a unique address by your service provider. This address is linked to the real world location of the computer or device you use. Law enforcement can access your unique address, which is linked to every communication you send online

- Remember to be a good friend and remind your friends if they are behaving inappropriately that they are not anonymous and can be traced

- Copyright refers to the protection given to authors, which protects them against unauthorised copying of their work. Copyright can be attached to text, music, pictures and video clips. Check carefully for the copyright status of content prior to download or sharing. Violation of copyright can lead to very serious consequences

- You can use a Creative Commons to mark your creative work with the freedoms you want it to carry. You can use Creative Commons to change your copyright terms from "All Rights Reserved" to "Some Rights Reserved." It is important to consider what sort of protection you would like to give to your own content and to respect the Copyright protections linked to other users content

Respect the hood:

Online communities thrive on interactions that are interesting, funny and witty. It is important to contribute in engaging and relevant ways. Your images, video clips and comments that you share with others help to shape the online community and ultimately, can make it and all of its neighbourhoods a great place to 'hang out'. There are some basic points which will demonstrate your respect for the community as follows;

- Respect what other people contribute and the time and effort they have put into creating and sharing content

- The internet is a very public place so local or personal disagreements can spiral very quickly out of control and lead to very public humiliation, which can cause hurt and distress beyond what you ever intended

- If you become aware of any difficulties that other people are experiencing, for example, threatening, bullying or nasty behaviours, do not interact in ways which might worsen the situation – report it to your service provider and seek their help and advice

Just don't take it – reporting abuse and seeking advice and help

- If problems or difficulties arise within the community use the available tools to block, ignore, pre-screen or report inappropriate content or behaviours to the service provider

- Your service provider may have links to sources of expert help and advice (both online and offline), confidential help lines or support services on the Help / Customer Care / Report Abuse pages of the service

- On occasions the behaviour you experience online may warrant you contacting the police directly. If you or another young person you are in immediate danger and you require an urgent response, you must call 999 or your local police
- Speak to a trusted adult or friend if you are unsure about anything. It is always good to seek advice when you are unsure

APPENDIX D

Child Exploitation and Online Protection Centre (CEOP)

What is CEOP and what does it do?
CEOP has the legal remit and authority for tackling online child sexual abuse within the UK, as well as dealing with its offline consequences. Although primarily a law enforcement agency it has adopted a new holistic approach to this issue and looks to work proactively to tackle the problem, not just simply reacting when something has occurred. It is also a founder member of the Virtual Global Taskforce (VGT); the principle vehicle for international strategy and law enforcement action in this area of criminality. CEOP is affiliated to the Serious Organised Crime Agency (SOCA), but is operationally independent. It works closely with the Home Office on all aspects of tackling online and offline child sexual abuse.

CEOP provides a single point of contact for the public, law enforcement and the internet/communications industry to deal with reported allegations and suspicions of any online or offline activity or behaviour that suggests a child (under the age of 18) is being sexually abused by an adult or is at potential risk of such abuse. Policy and operational implementation for reporting mechanisms and subsequent activity in relation to child sexual exploitation has been delegated by the Home Office to CEOP. Currently, CEOP does not have the authority or the resources to deal with other forms of child abuse, such as bullying, harassment or racial abuse. It has a full web presence at www.ceop.gov.uk. It also has education and awareness resources aimed at children and young people; information on this can be found at www.thinkuknow.net.

How does CEOP get reports?

Information about online child sexual abuse can come into the CEOP in a number of ways. Principally these are:

- Public reporting - through the online “Report Abuse” mechanism, as well as telephone and written communications.
- Industry reporting – where industry, in the course of conducting its business, uncover suspicious behaviour/communications that may suggest online child sexual abuse.
- Referrals from law enforcement or child protection organisations, nationally and internationally.

Public Reporting

CEOP strongly encourages the public, particularly children and young people, to report directly to it. This is important because these are potential crimes and a law enforcement agency is best placed to analyse, assess and take appropriate action to safeguard an individual child.

It is working with industry partners to ensure that CEOP’s “Report Abuse” mechanism is placed and contextualised in prominent positions within environments that children and young people occupy online, so that links to the reporting page are as few as possible. CEOP recognises that each service is different and that a "one-size" fits all approach will may not succeed, therefore, will work with each industry partner (that adopts the CEOP "Report Abuse" mechanism) to ensure that it is placed within the best environment possible throughout the services they provide.

Industry Reporting

It is important for industry to be able to report directly to CEOP about concerns or behaviour that they come across in the course of their work or where a service user reports such behaviour or activity directly to them. During 2007 a bespoke system for industry to report concerns directly to CEOP will be in place.

Industry partners may have concerns about reports that are sent directly to CEOP about online behaviour or activity within their environment, but which they are not sighted on. CEOP recognises those concerns and, appreciates that feedback about those reports should be made available to industry to allow it to take action to deal with behaviour that is inappropriate, but not necessarily be serious enough to warrant criminal action, because it may have breached "terms and conditions of use" .

Handling Reports

All reports made online to CEOP/VGT will receive an automated response acknowledging receipt of that report and informing the author that someone from CEOP will contact them. All reports from someone under 18 will be followed up and replied to. Those who wish to make reports that are extremely urgent are advised to report directly to their local police force, using the '999' procedure.

Each report received by the Centre is risk assessed by professional and trained analysts to determine the course of action required and whether an urgent response is required. This risk assessment will inform whether a child is at immediate risk from sexual abuse and whether an urgent dissemination to a law enforcement or child protection agency is required. Working alongside those analysts are child protection staff from the NSPCC to help ensure that safeguarding of the child is put at the very heart of that assessment process.

All reports are monitored 24 hours a day, 7 days a week. For UK reports (made directly through the CEOP reporting mechanism) coverage for "out of hours", in the evenings and at weekends, is provided by "Crimestoppers" - where urgent action is required. Additional resilience is provided by VGT partners who have the ability to monitor on CEOP's behalf and contact CEOP staff 24/7. Those who may need advice or support before they make a report are directed to the NSPCC helpline if it is an adult, and Childline or the "There4me" website, if it is a child or young person.