

HOME OFFICE TASK FORCE ON CHILD PROTECTION ON THE INTERNET



Home Office

Good practice guidance for the providers of social
networking and other user interactive services 2008



2008

HOME OFFICE TASK FORCE ON CHILD PROTECTION ON THE INTERNET

**Good practice guidance for the providers of social networking
and other user interactive services 2008**

CONTENTS

| | |
|--|----|
| HOME SECRETARY'S FOREWORD | 3 |
| STATEMENTS OF SUPPORT | 5 |
| CONTRIBUTORS | 7 |
| PROJECT TEAM AND CONTRIBUTORS | 8 |
| PART 1: SOCIAL NETWORKING AND OTHER USER INTERACTIVE SERVICES | 9 |
| 1. Introduction | 10 |
| 2. The Internet and recent developments | 10 |
| 3. What are social networking sites and user interactive services? | 11 |
| 4. Why are social networking services popular with children and young people? | 11 |
| 5. How are social networking and user interactive services structured? | 12 |
| 6. Social networking, location and GPS services | 13 |
| 7. Premium-rate services | 14 |
| 8. Children's use of the Internet | 14 |
| 9. Bullying and harassment | 17 |
| 10. Self-harm and destructive behaviours | 17 |
| 11. Sexual exploitation of children and young people online | 18 |
| 12. The use of webcams and other technologies to sexually exploit children and young people | 19 |
| 13. The criminal law affecting personal interactions in interactive services | 20 |
| 14. The importance of education and media literacy in keeping children and young people safer online | 20 |
| 15. Age-verification and identity authentication | 21 |
| PART 2: RECOMMENDATIONS FOR GOOD PRACTICE | 23 |
| 1. General principles | 24 |
| 2. Safety information, awareness and education by service providers | 24 |
| 3. Editorial responsibility | 25 |
| 4. Registration | 25 |
| 5. User profile and controls | 27 |
| 6. Search | 28 |
| 7. Content screening and moderation | 28 |
| 8. Identity authentication and age verification | 28 |
| 9. Responsible use and managing bullying and other forms of abuse via communications technology | 29 |
| 10. Reporting concerns, abuse and illegal behaviour | 30 |
| 11. Relationships between service providers and law enforcement | 32 |
| PART 3: SAFETY TIPS | 33 |
| 1. Safety tips for parents and carers | 34 |
| 2. Safety tips for children and young people | 38 |
| APPENDICES | 41 |
| APPENDIX A: The criminal law | 42 |
| APPENDIX B: Children and the Internet | 46 |
| APPENDIX C: Child Exploitation and Online Protection Centre (CEOP) | 51 |
| APPENDIX D: Internet Watch Foundation (IWF) | 53 |
| APPENDIX E: NSPCC and Childline | 54 |
| APPENDIX F: Samaritans/Befrienders Worldwide | 55 |
| APPENDIX G: National Center for Missing & Exploited Children (NCMEC) and the CyberTipline | 56 |
| GLOSSARY | 60 |
| CHECKLIST | 64 |

HOME SECRETARY'S FOREWORD



I am delighted to launch this good practice guidance, which has been developed on behalf of the Task Force on Child Protection on the Internet.

The Task Force was established in 2001 and brings together

representatives of the Internet industry, mobile phone companies, law enforcement agencies, children's charities and government, who work together with the shared aim of making the Internet a safer place for children. The Task Force has previously produced good practice guidance for search service providers and for moderation of interactive services.

Internet services have recently taken a leap forward with the development of user interactive services, led by social networking providers and video-sharing websites. The take-up of these services has been extremely rapid. While some of these services have been developed specifically for children, many were aimed at older teenagers and adults but have attracted the attention of children who wish to use the Internet to maintain contact with current friends, make new friends or show their technical expertise in using modern communication tools.

The guidance has been drawn up with considerable input from many of the key industry providers, some of whom are based outside the UK, and I congratulate them for putting aside their commercial interests and working in a collaborative way to produce a series of recommendations which should help make the Internet environment a safer place for all. The development of the guidance has attracted international attention and it has received valuable input and support from the National Center for Missing & Exploited Children in the USA and from the Australian Communications and Media Authority.

I also want to offer particular thanks to the Child Exploitation and Online Protection Centre (CEOP) for its input into the guidance. The Government set up CEOP in April 2006 specifically to establish a proactive policing presence on the Internet, and the centre works tirelessly to tackle misuse of Internet services by individuals seeking to contact children for inappropriate reasons. Major children's charities including the NSPCC, NCH and Childnet have also contributed significantly to the recommendations drawn up in the guidance.

In the UK, the Government supports a self-regulatory model for the Internet industry. While the recommendations in this guidance are voluntary, the success of the guidance depends on a wide take-up of these recommendations within the industry. Self-regulation can only be effective when companies take the appropriate steps to help address concerns about child protection arising from the development of new services.

This document represents a tremendous achievement and shows a unique joined-up approach between government, children's charities, law enforcement and industry. I am very grateful to everyone for the time and effort they have put into developing the guidance.

I strongly urge industry providers to consider the recommendations in the guidance. I also recommend that parents and carers take note of the safety tips provided.

A handwritten signature in black ink, reading 'Jacqui Smith'. The signature is fluid and cursive, with a long horizontal stroke at the end.

Rt Hon Jacqui Smith MP
Home Secretary

STATEMENTS OF SUPPORT



The National Center for Missing & Exploited Children would like to applaud you for spearheading the creation of the “Good Practice Guide for the Providers of Social Networking and User Interactive Services.” This guide is an important step in helping to protect our children and teens as they communicate, connect, and share their interests with other users online. Providers of these services, which are increasingly popular among children and teens, will benefit from the recommendations given to empower their users to help avoid victimization.

Education plays a major role in keeping children and teens safer online and empowering them to make safer online choices. This good practice guide gives tips for parents and guardians to help teach their children and teens about the possible dangers and how to avoid them. Parents and guardians must be aware of their children’s online activities and become involved in their child’s online life.

NCMEC is excited to be a part of this collaborative project and we endorse this with our logo and full support. We encourage this guide to be used as resource for providers of social networking sites and user interactive services in helping to protect the children and teens who use their sites.

Thank you for spearheading this initiative,

Ernie Allen

President & Chief Executive Officer
National Center for Missing & Exploited Children



Australian Government
**Australian Communications
and Media Authority**

ACMA’S SUPPORT FOR THE GOOD PRACTICE GUIDANCE FOR THE PROVIDERS OF SOCIAL NETWORKING AND OTHER USER INTERACTIVE SERVICES 2008

Congratulations on the completion of the *Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services 2007*. We would also like to thank you for the opportunity provided to ACMA to participate in the drafting of the Guidance, through the direct participation of its staff.

It is ACMA’s view that the Guidance provides a sound framework for addressing safety issues associated with the use of social networking and other user interactive services. The Guidance also demonstrates the pleasing outcomes of a cooperative approach across jurisdictions with input from both government and industry interests.

Once again congratulations and thank you.

Yours sincerely

Lyn Maddock
Acting Chair
Australian Communications and Media Authority



The Child Exploitation and Online Protection Centre (CEOP) welcomes the publication of this guidance. This represents a good step forward towards the better online protection of children and young people. As the leading law enforcement unit in the UK with prime responsibility for protecting children online, CEOP looks forward to the full implementation of these guidelines on social networking and user interactive sites being used by children.

After our full participation in this project, CEOP looks forward to working closely with other stakeholders in ensuring that the Internet is an environment where children are protected from potential exploitation.

CONTRIBUTORS



vodafone



PROJECT TEAM AND CONTRIBUTORS

Chair: Annie Mullins – Vodafone (Global Head of Content Standards)

Secretary: Stephen Ruddell – Home Office/Ministry of Justice (Policy Advisor)

Graham Anderson – CEOP (Seconded from AOL UK)

Emma Ascroft – Yahoo! UK & Ireland (Head of Public and Social Policy)

Chris Atkinson – Fox Interactive Media/MySpace (Safety and Security Manager)

Maggie Brennan – CEOP (Research Development and Strategy Advisor)

Jo Bryce – Cyberspace Research Unit, University of Central Lancashire (Director)

John Carr – Children’s Charities Coalition on Internet Safety (Advisor, NCH)

Trish Church – Orange (Mobile and Broadband Services Safety Manager)

Julian Coles – BBC (Senior Advisor, Editorial Policy)

Keith Crowell – Piczo Inc (Director, Member Services)

Camille de Stempel – AOL (Director of Policy)

Cristina Fernandez – National Center for Missing & Exploited Children, USA

Will Gardner – Childnet International (Deputy Chief Executive Officer)

Alex Goodger – IWF (Internet Content Analyst)

Liz Harding – MSN UK (Community Affairs Manager)

Zoe Hilton – NSPCC (Policy Advisor)

Melissa Jordan – Australian Communications & Media Authority (Senior Policy Analyst)

Chris Kelly – Facebook (Chief Privacy Officer and Head of Global Policy)

Professor Sonia Livingstone – London School of Economics and Political Science

Hamish MacLeod – UK Mobile Broadband Group

Nancy McBride – National Center for Missing & Exploited Children, USA

Patricia Moll – Google/YouTube (European Policy Manager)

Alex Nagle – CEOP (Head of Harm Reduction)

Rachel O’Connell – Bebo (Head of Corporate and Social Responsibility)

Remco Pijpers – My Child Online, The Netherlands (Seconded from KPN)

John Shehan – National Center for Missing & Exploited Children, USA

Hon. Mozelle W Thompson – Thompson Strategic Consulting – Facebook

Contributors

Robert Beattie – Department for Children, Schools and Families (Policy Advisor)

Matt Colebourne – Lunarstorm (UK CEO)

Paul Cording – Vodafone Global Content Standards (Senior Manager)

David Evans – Information Commissioner’s Office

Lynda Jackson – Home Office/Ministry of Justice (Senior Policy Advisor)

DCS Alistair Jeffrey – Metropolitan Police (Child Abuse Investigation Command)

Matt Lambert – Microsoft (Director of Corporate Affairs)

Anthony Langham – UK Samaritans (Public Affairs Manager)

Justin Millar – Home Office (Policy Advisor)

Julie Minns – Hutchison 3G (Head of Content and Consumer Regulation)

Hemanshu Nigam – Fox Interactive Media/MySpace (Chief Security Officer)

Dr Anna Stacey – Department for Business, Enterprise and Regulatory Reform

DI Brian Ward – Metropolitan Police (Child Abuse Investigation Command)

Vicky Wood – Department for Children, Schools and Families (Policy Advisor)

PART 1

Social networking and other user interactive services



1. INTRODUCTION

PURPOSE OF THIS GUIDANCE

Social networking and user interactive services offer many positive opportunities for children and young people to communicate, interact, and share content and interests. However, children and young people (under the age of 18) may also be vulnerable to inappropriate or harmful contact through these services. As in the real world, there is no environment that is completely safe. Co-operative efforts between business, government, law enforcement and users can help create a safer, more secure online environment for children and young people. This task begins by making them aware of the possible risks and continues by providing them with tools and safety measures designed to help them manage their online experience and to protect themselves from potential harm.

This document has been produced to provide good practice recommendations for the providers of social networking and other user interactive sites, to enhance the safety of children and young people using their services.

The guidance also seeks to:

- describe the evolution of the Internet in respect of social networking and other user interactive services;
- highlight potential risks and safety concerns; and
- provide industry and others with safety advice and tips for children and young people, and their parents and carers, to use as they wish.

STATUS OF THE GUIDANCE

Generally speaking, the criminal law applies equally to the Internet as elsewhere and what is illegal offline is illegal online. In addition, the UK Government supports and encourages industry to work within an effective self-regulatory framework, and this good practice model for social networking and interactive services is the latest example of this approach.

It is recognised that the communications and Internet industry is very diverse and ranges from large global providers to small locally run services, so the guidance is not a 'one size fits all' solution. Providers are responsible for how they deliver their services. In determining the actions they should take, providers will need to take into account the particular nature of their services so that they can apply the relevant recommendations of this guidance. It is for them to judge where and how far to apply any specific point in the guidance.

The intention is that service providers, of whatever size, utilise the guidance to enhance the safety of children and young people using their services. This guidance is not intended to be prescriptive or legally binding, but is offered to service providers with a strong recommendation for its use.

2. THE INTERNET AND RECENT DEVELOPMENTS

The World Wide Web has evolved to become an increasingly dynamic and interactive medium.

Social networking and user interactive services are now hugely popular and have become a compelling activity for many Internet users. These services are 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, download of content, use of search engines, and surfing from one website to the next. However, Web 2.0 represents a fundamental shift away from this model, towards a more dynamic and interactive Internet, where content is generated by users, uploaded and shared easily with others and within communities.

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, personal digital assistants (PDAs), game consoles and PCs. This means that users can interact with each other and post and download content on many different services and devices.

3. WHAT ARE SOCIAL NETWORKING SITES AND USER INTERACTIVE SERVICES?

Social networking sites allow users to create their own content and share it with a vast network of individuals, and potentially with the world. There is now a proliferation of these services, and user-generated content has taken hold in mainstream culture, due to its authentic and original appeal. Some examples of popular services include: Bebo, CyWorld, Facebook, Faceparty, Flickr, Friends Reunited, Hi5, LinkedIn, MySpace, Piczo, Windows Live Spaces, Xanga and Yahoo! 360°. Other services focus on particular features or themes, such as sharing video (e.g. YouTube, Daily Motion, AOL Uncut, Grouper, iFilm, Google Video and SeeMeTV), but have similar characteristics to social networking services, such as having a user profile and the ability to interact with others.

In one sense, social networking is nothing new. These services, for the first time, simply bring together pre-existing interactive technologies on a single service. These technologies and tools can include all or some of the following: search, email, messaging, chat, blogs, gaming, discussion forums, Voice over Internet Protocol (VoIP), photos, music and videos.

There are a vast number of social networking and user interactive services worldwide, and new ones are being launched almost daily, making it difficult to quantify the sector. Wikipedia, for example, currently lists approximately 100 services that operate on a global or local basis.¹ The services vary in terms of audience, features and the range of activities that users can engage in. These services can allow users to:

- create and design a personal website using graphics, colour, music and images to represent the user's unique style and identity;
- interact with friends in real time through instant messaging, message boards and chat rooms that are integrated into the sites;

- meet known friends and make new friends;
- link to friends' personal websites;
- upload and share images of themselves, their family and friends;
- upload and share videos;
- create blogs, journals or diaries about their lives;
- publish and share their own music;
- share thoughts and information on areas of interest;
- play online games;
- receive comments or messages on their personal websites from friends or guests;
- create or join wider communities or interest groups, e.g. football or music; and
- complete or create questionnaires integrated into some social networking sites.

Interactive services have also developed around specific communities of interest that are very popular with children and young people. These share many of the characteristics of social networking and include online gaming communities, such as Runescape and World of Warcraft, and virtual worlds, such as Second Life and Habbo Hotel.

Children and young people are also engaging in auctioning and trading, for example in communities such as Swapits, which has a virtual global currency where young people can earn rewards, trade and shop. All these communities encourage and facilitate social interaction.

4. WHY ARE SOCIAL NETWORKING SERVICES POPULAR WITH CHILDREN AND YOUNG PEOPLE?

There are many reasons for the appeal of social networking services. One of the key attractions includes the ability to create original and personal content that can be published in the form of a website. Perhaps most importantly are the opportunities for children and young people to express themselves through these services and to connect and communicate easily with others.

¹ http://en.wikipedia.org/wiki/List_of_social_networking_websites

Key activities include:

- keeping in touch with friends and sharing interests;
- experimenting with their identity and opinions;
- having a ‘place’ or ‘space’ where their parents or carers may not be present; and
- demonstrating their technical expertise and skill.

Children and young people use social networking and interactive sites as an extension of their offline lives, and many do not distinguish between the online and offline environments.

5. HOW ARE SOCIAL NETWORKING AND USER INTERACTIVE SERVICES STRUCTURED?

MINIMUM AGE AND THE US LEGAL FRAMEWORK

Many social networking and interactive services available to users in the US, the UK, Australia and other jurisdictions share some common characteristics. In particular, many service providers have set 13 years as the minimum age at which a young person can register as a user of the service. Some services also use a range of technical tools to try and prevent users under the age of 13 years from registering and accessing their service.

It is important to note that in the UK, Australia and elsewhere there is no legal reason why 13 years should be the minimum age. The reason why many service providers operating in the UK and other jurisdictions choose this as their minimum age lies in the fact that many are US-based companies and must comply with several US laws which designate the age of 13 as that which distinguishes children from teenagers and young adults. These laws include the Children’s Online Privacy Protection Act (COPPA) 1998² for companies that offer services in the US and overseas and knowingly collect personal information from children. COPPA aims to protect children’s personal information, by placing a number of requirements on US commercial providers, including only allowing users over 13 years of age to register for a service without parental consent.

² www.ftc.gov/privacy/coppafaqs.shtm

Service providers may also be required to comply with additional local legal requirements pertaining to children’s privacy, which may affect how the service is operated in any given jurisdiction. In the absence of specific local legal requirements, however, service providers will generally adopt the original US product design in all markets and provide all users with the same protections.

CHILDREN’S PRIVACY

In the UK, organisations which process information relating to living, identifiable individuals are required to comply with the provisions of the Data Protection Act 1998. The Act makes no distinctions based on age, and children have the same rights as adults (for example, the right to access personal information and the right to request that information is not processed where processing is likely to cause substantial damage or distress). In practice, there will be occasions when a parent or guardian acts on behalf of a child because the child is not capable of understanding how to exercise their rights but, overall, it should be remembered that children enjoy the same rights and are afforded the same protection as adults.

Indeed, there is a strong argument that service providers need to take extra care when processing information³ about children, to ensure compliance with the Act. For example, there is a requirement that processing has to be ‘fair’. Fairness often involves explaining to individuals how, why and by whom information about them will be used. Service providers should ensure that the information they provide to children and young people is appropriate for the user age group – what might be within the reasonable expectations of, and fair to, adults, might not be apparent or fair to children. In addition, privacy-friendly options available to children and young people should be well signposted and easy to use for the collection of information to be fair.

³ www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/issues_paper_protecting_childrens_personal_information.pdf
See also: www.ico.gov.uk/Youth.aspx

Additionally, to be confident that information is held securely, service providers should consider providing more information to children about the security features available, such as how to choose a suitable password.

INDUSTRY APPROACH

Service providers already use a number of systems to deny access to users who declare they are under 13 years of age, and they also act against children who misrepresent their age to gain access to a service, for example by:

- placing a ‘cookie’ onto a user’s computer to prevent the user from attempting to re-register with false age details;
- using technical tools such as search algorithms to look for slang words typically used by children and young people and to identify children under 13 years old who may have lied about their age at registration; and
- offering free downloadable parental controls which allow parents to manage their children’s use of the service (see safety tips for parents and carers in Part 3).

It is important to note that service providers work within the limits of current technology. While these solutions help to prevent abuse of social networking services and help to protect children and young people from inappropriate contact and content, they are not foolproof. Determined children and young people can bypass some technical solutions. It is therefore important to continuously improve these tools, as well as supplementing them with user education. We discuss this in more detail in section 14.

6. SOCIAL NETWORKING, LOCATION AND GPS SERVICES

At the time of publication of this guidance, a small number of social networking sites are being developed to work with mobile services, using customers’ real-time location. These are being marketed as a service for determining the whereabouts of friends and keeping in touch with them.

Location data can be provided through a variety of technical means: GPS-enabled⁴ mobile devices; data supplied by the mobile networks based on cell sites; and, for Wi-Fi-enabled devices, data from a network of Wi-Fi hotspots. Some services can combine data from more than one source.

The processing of location data is covered by legislation such as the E911 Act in the US and the Privacy and Electronic Communications Regulations in the UK.⁵ Under section 14 of the latter, location data can only be processed by a service provider with the consent of the person being located. Such consent must also be capable of being withdrawn by the customer at any time. ‘Processing is used to describe any action or series of actions or operations that computer and communication technologies carry out in relation to the data supplied to them.’⁶

UK location service providers that derive data from the mobile networks are also governed by a *Code of Practice* developed by the industry and published in 2004.⁷ Among other things, the Code requires: locators to have their identity and address verified; parents to give consent if the person being located is under 16; and regular reminders to be sent to the mobile devices to remind customers that their phone can be located.

Customers are very sensitive about giving away their location. Only those services that carefully respect customers’ rights to protect their privacy will be successful. If social networking sites are to integrate real-time location information, and that service is to be made available to legal minors, the Government will need to consider any potential concerns about the possibility of inappropriate or unauthorised contacts.

⁴ Global Positioning System – a GPS-enabled mobile device can determine its position based on timing supplied by a constellation of geo-stationary satellites. Accuracy can be up to a few metres, providing the mobile device is outside and has line of sight to the satellite(s).

⁵ The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI No 2426).

⁶ Walden, I. (2007), *Computer Crimes and Digital Investigations*, Oxford University Press, paragraph 2.16.

⁷ www.mobilebroadbandgroup.com/social.htm

7. PREMIUM-RATE SERVICES

Providers of social networking services are reminded that where they use premium rate to charge for any aspect of the service (such as Premium SMS) in the UK, then the service, and its related marketing, will also need to comply with the Code of Practice for phone-charged services which is approved by Ofcom and administered by PhonepayPlus. The Code sets out a number of general rules about the advertising and marketing of services, as well as the actual operation of the service. Providers are particularly reminded that PhonepayPlus has specific rules which apply to services that are aimed at, or would be particularly attractive to, children (defined as those under 16 years old). Among the rules relating to children, PhonepayPlus specifies that children's services should not cost more than £3, or in the case of subscriptions, no more than £3 per month. The PhonepayPlus Code of Practice can be downloaded at www.phonepayplus.org.uk. PhonepayPlus offers an online compliance advice service (compliance@phonepayplus.org.uk) or can be contacted by telephone at 0845 026 1060. Calls to this number cost 4p per minute; network extras apply.

In addition, all advertising of the premium-rate service will need to comply with the British Code of Advertising, Sales Promotion and Direct Marketing (www.asa.org.uk/cap/codes/) as well as the BCAP radio and TV codes. Marketers should ensure that advertisements for premium-rate services are not misleading by omission and that they make clear the cost of calls. Marketers should also take special care when addressing advertisements for premium-rate services to children.

8. CHILDREN'S USE OF 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,⁸ has been conducting leading research in the UK about children and young people's use of the Internet. Her report, *UK Children Go Online*, gives an important insight into children and young people's use of the Internet which is relevant to this guidance.⁹ This is important as a context for understanding the risks to children and young people online. A summary of the main findings is available in Appendix B.

While this research pre-dates the mass take-up of social networking services, many of the current dimensions of children and young people's Internet use are still relevant in this new environment. It is nevertheless vital that research continues to enhance our understanding, particularly as use of social networking is now much more commonplace among this age group.

ADOLESCENT SOCIAL AND SEXUAL DEVELOPMENT AND MATURITY

It is a normal part of adolescence to test boundaries, challenge adult norms, experiment with relationships, play with identities, explore new sexual experiences, keep or break secrets, exclude or be excluded by peers, deceive parents and worry about one's development. All this is to be expected online, as it is 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.

‘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.’¹⁰

⁸ www.lse.ac.uk/collections/media@lse/whosWho/soniaLivingstone.htm

⁹ Following qualitative interviews, observations and focus groups, the main part of this Economic and Social Research Council-funded project consisted of 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.

¹⁰ Lorie, 17, from Essex, interviewed by the UK Children Go Online project (see above).

This quote captures the growing consensus¹¹ 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.¹²

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. Another view is that children are competent and creative agents in their own right, whose 'media-savvy' skills tend to be underestimated by the adults around them, with the consequence that society may fail to provide a sufficiently rich environment for them. Finding a position that recognises both characteristics is important.

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 test themselves against, and learn from, more complex

experiences.¹³ The influence of the peer group grows in importance during adolescence, as the influence of parents declines (although remaining substantial).

US PERSPECTIVE

According to Dr Sharon Cooper, CEO of Developmental and Forensic Pediatrics, PA – a consulting firm that provides medical care, training, and expert witness experience in child maltreatment cases – the prefrontal part of the brain that controls reason, emotion, common sense and judgement does not mature until nearly the age of 21 years.¹⁴

Pew Internet and American Life Project is a US research institute that produces reports exploring the impact of the Internet on families, communities, work and home, daily life, education, healthcare, and civic and political life. The project aims to be an authoritative source on the evolution of the Internet through collection of data and analysis of real-world developments as they affect the virtual world.

Pew has produced a number of valuable reports which give critical insights into how children and young people are using the Internet, including some of the difficult issues arising, such as bullying. One 2007 survey found that among the 55% of online American 12–17 year olds who use social networking sites, most are successfully balancing the sharing of personal information with trusted friends, while also revealing enough about themselves to make new friends online.¹⁵

¹¹ As argued by the recent review by End Child Prostitution, Child Pornography and the Trafficking of Children (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.

¹² 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).

¹³ A fair summary of child development is provided in the table on pp.116–17 in Thornburgh, D. and 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.

¹⁴ www.netsmart.org/safety/videos/dr-development.htm

¹⁵ Lenhart, A. and Madden, M. (2007), *Social Networking Websites and Teens: An Overview*. Pew Internet and American Life Project Memo, 1 July 2007. Available at: www.pewinternet.org/PPF/r/198/report_display.asp. The study notes that: 'For girls, social networking sites are primarily places to reinforce pre-existing friendships; for boys, the networks also provide opportunities for flirting and making new friends'.

Several difficulties can arise from using social networking services:

- responding to contacts from strangers;
- deciding who is a 'friend'; and
- setting the controls so as to manage what is private and what is public.

The Pew survey found that: most (66%) keep their profile wholly or partially private; of the information that is public, most is either non-revealing or false; and only half (49%) claim to make new friends through social networking, most preferring instead to use social networking to contact those who are already friends. Since the number of contacts is considerable – a 2006 US Harris Interactive survey of 1,487 8–18 year olds found that among 13–18 year olds, the average number of social networking 'friends' is 75, with many having hundreds of contacts – the benefits and risks are both sizable.¹⁶

Indeed, the Pew survey found that, of the 32% who have been contacted by strangers online, 23% (i.e. 7% of all online teenagers) felt scared or uncomfortable about that encounter. Not all teenagers are the same, however, with boys and younger teenagers being more likely to post false information, while older teenagers – especially girls – are more likely to reveal detailed personal information.

RISKS TO CHILDREN AND YOUNG PEOPLE ONLINE

Most children and young people use the Internet positively but sometimes behave in ways that may place them at risk. Some of these actions to them seem harmless but could expose them to potential harm. In addition, some of these risks do not necessarily arise from the technology itself but result from offline behaviours that are extended into the online space. A young person can be a victim of online abuse through exposure

to harmful content and cyberbullying. Young people may also engage in behaviour that is risky to themselves, including cyberflirting and cybersex. These situations can quickly escalate to a point where the young person may lose control.

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

- bullying by peers and people they consider 'friends';
- exposure to inappropriate and/or harmful content;
- involvement in illegal or inappropriate content;
- posting personal information that can identify and locate a child offline;
- theft of personal information;
- sexual grooming, luring, exploitation and abuse through contact with strangers;
- exposure to information and interaction with others who encourage self-harm;
- exposure to racist or hate material;
- encouragement of violent behaviour, such as 'happy slapping';¹⁷
- glorifying activities such as drug taking or excessive drinking;
- physical harm to young people in making video content, such as enacting and imitating stunts and risk-taking activities; and
- 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, now or in the future. While social networking services offer great opportunities for children to be creative and express themselves online, they are often unaware that their words or images, although intended for a small audience, can quickly attract a far larger one and may have a lasting impact

¹⁶ Harris Interactive (2006), *Teens Set New Rules of Engagement in the Age of Social Media*, 31 October 2006 (survey conducted by Harris Interactive, summary of findings). Available at: www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=1114.

¹⁷ '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 attack unsuspecting children or passers-by while capturing the attacks on camera or videophones.

on other people's perception of them. Some individuals have become notorious as a result of their online postings, which have had both negative¹⁸ and positive impacts on their lives.

9. BULLYING AND HARASSMENT

Individual and group disputes are more often than not an extension of arguments and tensions that originate in the offline world. It is therefore no surprise that bullying and harassment are concerns for the children and young people who use social networking and user interactive services. It can manifest itself in the following ways:

- **personal intimidation** – posting personally abusive and threatening comments on the victim's or other people's website, blog or profile;
- **impersonation** – setting up fake webpages that are attributed to the victim of bullying, and may involve the publishing of manipulated pictures and comments;
- **exclusion** – blocking an individual from a popular group or community, deleting them from friendship lists, and/or using 'ignore functions';
- **posting images of bullying incidents** – users sharing and posting images or videos of victims being abused or humiliated offline;
- **stealing a password to take over a user's website** – to post comments and images which are attributed to the original user; and
- **making false reports to the service provider** – reporting other users for a range of behaviours with a view to having the user's account or website deleted.

Bullying in any form is distressing. With the proliferation and use of technology by children and young people, victims may feel they cannot escape and perpetrators may believe, falsely, that they are anonymous.

Bullying via communications technology and victimisation has the potential to be witnessed by a wide audience if it is recorded and shared on the Internet. This may extend the humiliation and

embarrassment of the victim. It is difficult to stop abusive content spreading and reappearing, as it can be easily and widely distributed on the Internet. Some victims may therefore find it difficult to manage or recover from the abuse, particularly if they do not know who the aggressor is.

As well as young people bullying their peers, some adults (particularly teachers) have also found themselves targets of online abuse and harassment. This has caused some concern within schools, not only about the individuals depicted in postings but also the reputation of the school. In some instances, these situations have resulted in investigations being initiated by law enforcement and education authorities. However, students' comments about their teachers' behaviour may not necessarily be abusive, but a form of normal self-expression about their experience in school, both positive and negative.

This emphasises the need for both parents and teachers to communicate to children and young people, and educate them about, the appropriate and responsible use of the Internet. Much work is being undertaken to establish school anti-bullying policies and to provide guidance and support to manage children's and young people's appropriate use of the Internet. In the UK, the newly formed Department for Children, Schools and Families (DCSF) Cyber-bullying Taskforce is developing guidance for schools, as part of an information campaign for children and advice for parents.¹⁹

10. SELF-HARM AND DESTRUCTIVE BEHAVIOURS

There has been longstanding concern about children and young people accessing websites, chat rooms and information forums that promote and/or incite risk-taking or dangerous behaviours, self-harm, suicide and eating disorders.

¹⁸ School pupils can receive disciplinary sanctions for posting images of bullying onto social networking sites.

¹⁹ See DCSF Cyberbullying Taskforce: www.dcsf.gov.uk/bullying/.

On social networking and user interactive sites, young people seek opportunities to inform one another and express themselves, and therefore may choose to upload content relating to these behaviours:

- eating disorders;
- dieting and body image;
- depression;
- drug and alcohol misuse;
- isolation and loneliness;
- bullying; and
- self-harm and suicide.

To the extent that it allows them to express their feelings and seek support, this can be a positive experience for young people dealing with life's challenges in this period of social development. They can seek out and create networks of like-minded young people who wish to explore these issues and access information. However, there can be negative or worrying aspects of this exploration and engagement which can manifest themselves in the apparent promotion or encouragement of self-harm, e.g. filming and publishing these activities.

It is important that providers promote opportunities for support and guidance for users related to the issues listed above by having links to helpful information and support organisations. In the event of a clear expression of intent to commit suicide, service providers should consider contacting the emergency services. In the UK, support organisations for children and young people include ChildLine²⁰ (free telephone helpline – 0800 1111) and the Samaritans (organisation for those with emotional distress, self-harm and suicide issues. See Appendix F).

11. SEXUAL EXPLOITATION OF CHILDREN AND YOUNG PEOPLE ONLINE

There is also concern that the capabilities of social networking services, combined with children's own high-risk behaviour, may increase the potential for sexual exploitation of children and young people by adults, or sometimes by other young people.

This exploitation can include:

- exposure to harmful content, including adult pornography and illegal child sexual abuse images;
- engaging in sexually explicit communications and conversations that may reduce children and young people's inhibitions;
- manipulation and exploitation, which can include being encouraged or paid to pose in sexually provocative ways and pose naked and/or perform sexual acts via webcams; and
- grooming and luring of children to meet offline to sexually exploit them.

THE 'GROOMING' PROCESS²¹

Grooming is a process by which someone makes contact with a child with the motive of preparing them for abuse either online or offline. Abusers can 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 contact taking place in the real world, for example by sending and exchanging sexual images, and/or by persuading children and young people to send explicit images of themselves. Abusers may also record young people performing sexual acts through webcams.

There have been a number of cases where adults have used social networking services as a means of contacting and grooming children and young people for sexual exploitation. In some cases, this has resulted in actual contact abuse. Abusers use a range of techniques to make contact and establish relationships with children and young people, including:

- gathering personal details, such as age, name, address, mobile number, name of school and photographs;
- offering opportunities for modelling, particularly to young girls;
- promising meetings with pop idols or celebrities, or offers of merchandise;
- offering cheap tickets to sporting or music events;

²¹ See NSPCC information and advice to parents: www.nspcc.org.uk/helpandadvice/publications/leaflets/protecting_children_pdf_wdf36296.pdf

²⁰ www.childline.org.uk/pdfs/info-self-harm.pdf

- offering material gifts, including electronic games, music or software;
- offering virtual gifts, such as rewards, passwords and gaming cheats;
- suggesting quick and easy ways to make money;
- paying young people to appear naked and perform sexual acts via webcams;
- gaining a child's confidence by offering positive attention and encouraging the child to share or talk about any difficulties or problems at home, and providing 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 saying they know where the child lives or goes to school;
- using webcams to spy and take photographs and movies of victims;
- asking sexually themed questions, such as 'Do you have a boyfriend?' or 'Are you a virgin?';
- asking children and young people to meet offline;
- sending sexually themed images to a child, depicting adult content or the abuse of other children;
- masquerading as a minor or assuming a false identity to deceive a child; and
- using school or hobby sites to gather information about a child's interests, likes and dislikes.

Having made contact with a child or young person, abusers may also use that young person as a means to contact and get to know their friends by using the links to their 'friends' in user profiles.

Whatever its guise, the grooming process can result in many young victims feeling guilty and responsible for inappropriate interactions, exploitation and actual abuse. They can find it extremely difficult to seek help or disclose their abuse because of their sense of personal responsibility, feelings of guilt or shame, and fear that they may not be believed or may be 'blamed' and lose access to the Internet. In some cases they may not identify the experience itself as abuse.

Often the child's feelings may be manipulated, so they genuinely believe they are 'in love' with the abuser.²²

12. THE USE OF WEBCAMS AND OTHER TECHNOLOGIES TO SEXUALLY EXPLOIT CHILDREN AND YOUNG PEOPLE

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

- they may be intimidated or manipulated into recording explicit images of themselves using webcams and sending them to individuals they first meet online. This allows these individuals to build libraries of images and videos of young people who might then be coerced into further contact by threats that the material may be published or revealed to their family and friends; and
- they may use the Internet to explore their sexuality and engage in cyberflirting or cybersex 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 child or young person may be classified as an illegal image of child abuse, 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 by the My Child Online Foundation in 2006, involving 10,900 participants between the ages of 13 and 19, reveals that 47% of girls who responded to the survey, said they had received unwanted requests to do something sexual in front of a webcam – although only 2% actually did so.²³

²² Ybarra, M. L., Mitchell, K. J., Finkelhor, D. and Wolak, J. (2007), Online Victimization of Youth: Five Years Later. *Journal of Adolescent Health*, 40, 116–26 (CV135). Available at: www.unh.edu/ccrc/pdf/CV138.pdf.

www.netcaucus.org/events/2007/youth/resources.shtml
www.unh.edu/ccrc/pdf/CV138.pdf

²³ <http://mijnkindonline.web-log.nl/mijnkindonline/2007/03/index.html> (report is not available in English).

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 over victims. This may involve gaining remote access to computers, accessing personal data and controlling webcams.²⁴

It is essential that Internet safety and education programmes include appropriate warnings and advice about the potential misuse of webcams and other technologies to manipulate and abuse children and young people.

13. THE CRIMINAL LAW AFFECTING PERSONAL INTERACTIONS IN INTERACTIVE SERVICES

It is important to note the general principle that an action that is illegal if it is committed offline is also illegal if it is committed online. This applies both to issues such as distributing illegal material and also to harmful behaviour, if it amounts to a course of harassment, or grooming. Inciting someone to commit an offence is also no less an offence simply because it is done through a computer or mobile phone. No-one using an interactive service should be under the illusion that the criminal law does not apply to what they do online. While the UK considers anyone under the age of 18 to be a 'child', some aspects of the criminal law, particularly with regard to behaviour such as grooming towards young people, will only apply to those under the age of consent, which is 16. More detail on the criminal law and its application to behaviours on social networking sites is available at Appendix A.

14. THE IMPORTANCE OF EDUCATION AND MEDIA LITERACY IN KEEPING CHILDREN AND YOUNG PEOPLE SAFER ONLINE

Education and media literacy form a critical part of keeping children and young people safer online and empowering them to manage their online experience. Responsible Internet use and online safety are considered essential life skills for children and young people. Research shows²⁵ 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 parental control tools are more likely to be installed on the home computer. 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.

Public bodies also play an important role. In the UK, for example, the Child Exploitation and Online Protection Centre (CEOP) has launched a national campaign 'Think U Know'.²⁶ 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.

In the US, NetSmartz,²⁷ a programme of the National Center for Missing & Exploited Children, gives parents, guardians, educators and law enforcement a variety of resources for learning and teaching the possible dangers of the Internet, and how to avoid them, to children and teenagers.

It is vital that parents and carers become involved in children's and young people's use of the Internet, including social networking and other user interactive services. It is critical that they have

²⁴ See, for example: <http://news.bbc.co.uk/1/hi/england/derbyshire/6133360.stm>.

²⁵ See Ofcom's *Media Literacy Audit: Report on media literacy amongst children* at: www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/children/.

²⁶ www.thinkuknow.co.uk

²⁷ www.netsmartz.org

direct conversations, particularly with teenagers, on a regular basis about what they are doing online, who they are communicating with and their experiences. A key focus for parents and carers must be how to understand not only what their children are viewing and downloading, but what information they are publishing online about themselves and others, including any text, photos or video.

This document provides important advice and guidance that should be shared with young people and their parents and carers. (Part 3 outlines some basic safety tips for parents, carers and young people.)

There is also a wide range of information and advice available both from service providers and from other organisations such as educational bodies and child welfare charities. We recommend the following key sites for information and advice:

- www.thinkuknow.co.uk (UK)
- www.netsmartz.org (US)
- www.netaert.net.au (Australia)
- www.internetsafetyzone.co.uk
- www.childnet-int.org/blogsafety
- www.blogsafety.com
- www.getnetwise.org
- www.nch.org.uk/information/index.php?i=135
- www.nspcc.org.uk/helpandadvice/parentsandcarers/safesurfing/safesurfing_wda35959.html
- www.childline.org.uk
- www.samaritans.org
- www.bbc.co.uk/chatguide/
- www.wiredsafety.org (US)

15. AGE-VERIFICATION AND IDENTITY AUTHENTICATION

The ability to obtain a verifiable identity, and therefore an age, for a user can be a useful tool in providing a safer and more secure environment for

children and young people on social networking sites and the Internet. However, there are significant challenges to the development of a comprehensive and reliable age-verification system arising from issues around data (e.g. a lack of a complete database of all Internet users) and technical and legal issues (e.g. data protection and privacy laws). If an effective age-verification mechanism were to be developed, it could serve several purposes, for example to segregate people registered as being under 18 years of age from adult users and to restrict access by those aged under 18 to adult or other age-inappropriate content services.

Notwithstanding the challenges mentioned above, there are a number of solutions and strategies being developed or evaluated to verify the age of adults using online services. These rely on checking registration information in real time against different data sources (usually more than one), such as the electoral register and data held by credit rating agencies. Developing similar approaches to age-verify under-18s, however, presents even greater challenges, as there are limited data sources on children available to industry that can be checked remotely and in real time. Some suggested solutions would rely heavily on an element of offline verification by parents, schools or another trusted party. This two-part approach poses both the challenge of authentication of the parent, school or trusted party and legal hurdles in some countries.

The challenge of protecting children and young people on social networking and other online services has stimulated research into solutions specifically designed to age-verify under-18s. Whether or not these solutions could be deployed by a particular service provider depends on a range of factors, including:

- ease of use by children and young people;
- level of ‘false positives’;
- length of time that verification takes;
- scalability for very large numbers of users;

- ability to deploy a single solution over multiple markets;
- technical compatibility with the provider's network; and
- the ability of ill-intentioned people/criminals to manipulate the systems.

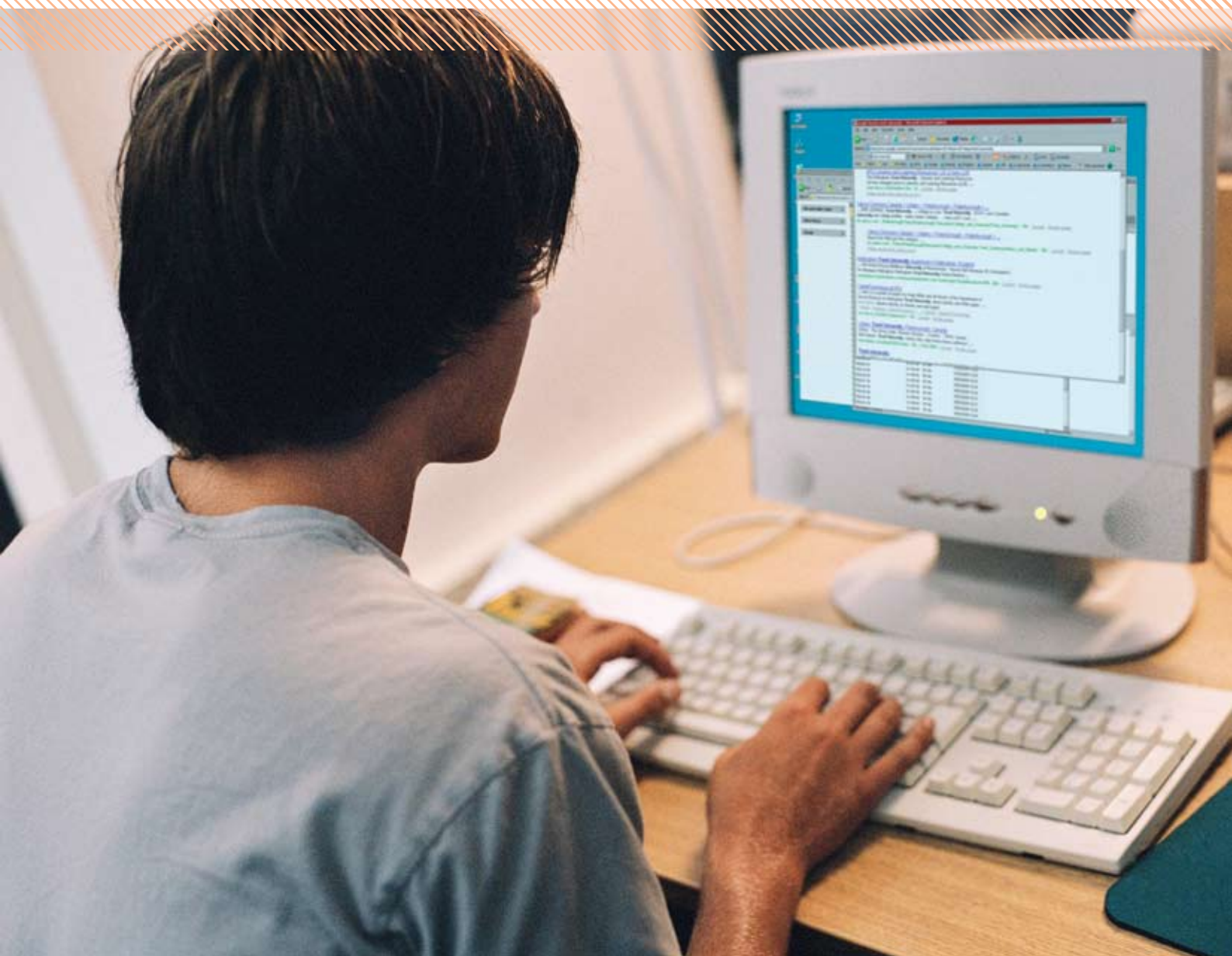
Individual service providers are engaging in trials to test the effectiveness of age-verification/identity-authentication mechanisms, but in the meantime, service providers continue to use a range of existing methods to safeguard children and young people using their service. These include

- promotion of confirmed affiliation with real-world communities, e.g. schools;
- user self-declaration;
- PIN protections;
- proof of account ownership;
- parental monitoring software; and
- verifiable parental consent.

These vary in their robustness, but in combination with other technical tools or human moderation they can enhance the protection of younger users of these services.

PART 2

Recommendations for good practice



The following recommendations provide good practice guidance to service providers to support a safer environment for young users.

1. GENERAL PRINCIPLES

- 1.1 These recommendations apply to all platforms, fixed and mobile, while recognising that the different characteristics of each platform (for example, the different screen sizes and methods of navigation) may require modified or alternative approaches to safety.
- 1.2 Each of the recommendations below should be included as part of a larger focus on user protection by responsible online sites. None of them should be viewed as a panacea.
- 1.3 Language and terminology should be accessible, clear and relevant for all users, including children, young people, parents and carers, especially in relation to the site's terms and conditions, privacy policy, safety information and reporting mechanisms.
- 1.4 When developing new services, providers should consider existing good practice guidance produced by the UK Home Office Task Force on Child Protection on the Internet for *Chat, Instant Messaging, Web Based Services, Moderation and Safe Search*.²⁸

2. SAFETY INFORMATION, AWARENESS AND EDUCATION BY SERVICE PROVIDERS

GENERAL

Online social networking and interactive services can provide extensive benefits to their users. However, the provision of safety advice by service providers for users of social networking and interactive services is critical. While children and young people will want to make the most of these services, they also need to understand the importance of protecting themselves, their online identities and their reputations.

RECOMMENDATIONS

Service providers should:

- 2.1 Make safety information for users, parents and carers, prominent, easily accessible and clear (see Part 3).
- 2.2 Offer links to relevant online resources that provide users with additional information about online safety and security.
- 2.3 Address personal safety issues but also individual responsibilities to respect and protect the wider online community, such as how to behave responsibly when posting images and comments.
- 2.4 Provide information which is:
 - specific to the service being provided;
 - updated to reflect service development; and
 - effective and relevant for users.
- 2.5 Make safety information available during the registration process, prominent from the homepage and in appropriate places within the service (e.g. in a welcome email/message).
- 2.6 Include instructions for tools which can help protect the user to maintain their privacy and prevent unwanted contact or communication, such as:
 - 'Ignore' functions;
 - removing people from their 'friends' or contact list; and
 - how to review and remove unwanted comments on their site.
- 2.7 Include instructions on how to make a report or complaint to the service provider, or elsewhere as appropriate.
- 2.8 Have in place robust procedures for handling complaints. In particular, complaints about harassment and inappropriate content must be assessed promptly, and, if appropriate, the offending content must be removed within a reasonable time.

²⁸ www.police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

- 2.9 Include instructions on how users can cancel their account and remove their unwanted profile.

3. EDITORIAL RESPONSIBILITY

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

RECOMMENDATIONS

Service providers should:

- 3.1 Exercise care and judgement in how prominently they feature sites created by children and young people, such as their profiles being featured on the homepage and encouraging other users to visit.
- 3.2 Be particularly sensitive to the context in which younger users' sites are presented and avoid inappropriate juxtaposition. For example, a profile of a user under the age of 18 appearing next to another with an adult theme.
- 3.3 Ensure that advertising displayed on social networking services should be appropriate for the likely audience, to the extent known. If a service is aimed at, or likely to attract, users under the age of 18, providers must follow relevant local guidelines or codes for advertising to minors. In the case of the UK, this is the British Code of Advertising, Sales Promotion and Direct Marketing.²⁹

In Australia, it is the Australian Association of National Advertisers Code for Advertising to Children.³⁰

- 3.4 Ensure that advertising displayed on social networking services within the European Union is compliant with the Unfair Commercial Practices Directive. (www.berr.gov.uk/consumers/buying-selling/ucp/index.html)

4. REGISTRATION

Registration is an important first step for authenticating user identification and promoting responsible behaviour online. During the registration process, users are asked to provide a certain amount of personal data and agree to the terms and conditions.

RECOMMENDATIONS

Service providers should:

- 4.1 Provide clear information about how details collected in registration will be used, including what information will appear on their profile, what will be public, and what will be private. Users should then be given the opportunity to hide, limit availability to, or edit this information.
- 4.2 Meet their legal obligations in respect of the amount of personal information collected from minors at registration, including obtaining informed consent.³¹
- 4.3 Carefully consider the implications of automatically mapping across personal information disclosed during registration to the user's profile. In this instance users should be informed of this process to

²⁹ www.cap.org.uk/NR/rdonlyres/A44808F1-1573-482A-A0E5-D8045943DA57/0/The_CAP_Code_Ed11_20061205.pdf

³⁰ Australian Association of National Advertisers Code for Advertising to Children: www.aana.com.au/pdfs/A2CCode.pdf

³¹ In the UK – Information Commissioner's Office: www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/issues_paper_protecting_childrens_personal_information.pdf

afford them the opportunity to hide, limit availability to, or edit their personal information.

- 4.4 Consider emphasising, in accessible and easily understood language, **‘what behaviour is and is not acceptable on the service’**, particularly for young users and for their parents and carers. It is suggested that this information should be provided elsewhere in addition to its inclusion in the terms and conditions.
- 4.5 Emphasise to users that if they breach the terms and conditions of the service, the provider will take action, including co-operation with law enforcement agencies and other authorities if necessary. By highlighting that users’ activity is traceable, it may be possible to counteract the common misconception that they are anonymous or untraceable online and remind them that online actions may have offline consequences.
- 4.6 Where possible and appropriate, request and validate personal information from users, e.g. full name, date of birth and/or a valid email address. This is important, to minimise the risk of impersonation and enable service providers to protect younger users.
- 4.7 Capture an IP address or MSISDN or unique identifier (for mobile devices) with a date and time stamp at registration, regularly refreshed with repeated use of the service, including at each log-in, with a date and time stamp. This measure can improve the traceability of both registered and unregistered users (e.g. those leaving comments in a user’s guest book).
- 4.8 Consider placing a ‘cookie’ onto a user’s computer or capturing the MSISDN or unique identifier of a mobile device to identify a user who has tried to register as being below the minimum age, thus preventing them from attempting to re-register using a false age.
- 4.9 Set the default for full profiles to ‘private’ or to the user’s approved contact list for those registering under the age of 18.³² This may be difficult for services that have already been developed around the legal age of consent, e.g. 16 years. However, future services should strongly consider using 18 years. A setting to private should ensure that the full profile cannot be viewed or the user contacted except by ‘friends’ on their contact list unless they actively choose to change their settings to public or equivalent. Some service providers set the profile default as ‘private’ for all users.
- 4.10 The private default setting above may not be necessary where:
 - services are pre-moderated³³ by a trained moderator;³⁴ and
 - personal information in profiles is very limited, i.e. nickname used in place of actual name, general location, and personal interests only listed.
- 4.11 Prompt the user and require their consent before integrating or ‘scraping’ one or more existing address books, contact lists or ‘friends’ list (e.g. email or instant messaging). This should remain under user control, as a user may not necessarily wish for ‘friends’ approved in one service to also be ‘friends’ in a social networking service.
- 4.12 Consider reminding users to review their contact lists on a regular basis to ensure that their ‘profile’ is shared as they wish.

³² In the UK the age of consent is 16 and establishing contact with younger children (online or offline) in order to meet them at a later date for the purposes of engaging in sexual activity is an offence under section 15 of the Sexual Offences Act 2003.

³³ Pre-moderation enables service providers to ensure that inappropriate or contact information is not contained in user profiles, reducing the risk of unwanted contact.

³⁴ <http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce>

5. USER PROFILE AND CONTROLS

GENERAL

A profile is an easy-to-create webpage, where users can post personal information, including their name, email address, images and videos of themselves, friends and family, as well as interests and hobbies or other information that is relevant to them. It is therefore important that users fully understand what they are publishing for other users to view and how they can protect their privacy and personal data.

RECOMMENDATIONS

Service providers should:

- 5.1 Inform users in a prominent place what information they submit to their profile will be made public and what will be private. Users should be supported to understand the implications of the profile settings. For example, inclusion of a symbol (such as a lock or a key) may enable users to quickly identify the status of their personal details.
- 5.2 Inform users of the available options for how their profile or webpage can be searched by others either on the site or through search engines. The option of a public profile on the site which is not searchable via search engines should be offered to all users.
- 5.3 Provide warnings to users about uploading photos to their profile, for example: 'Photos may not contain nudity, violent or offensive material, or copyrighted images. If you violate these terms, your account may be deleted.'
- 5.4 Be careful not to encourage users, especially those under the age of consent, to disclose excessive personal data. Consider carefully what data fields are appropriate.
- 5.5 Provide advice to users about the implications of posting certain information – both from a safety and responsible use perspective. For example, the implications of posting or using:
 - personal data which may identify their home address, especially in open profiles;
 - images which contain location information, especially in open profiles;
 - images of other people without first obtaining their permission; and
 - inappropriate user names and images.
- 5.6 Inform users and make it as clear as possible what options users have to adjust privacy settings and to manage 'who sees what' and whom they interact with. For example, these settings could include features which allow users to select who can leave comments or post content on their pages. Consider making privacy settings available for all aspects of the service for such things as journals, blog entries, image galleries and guest books.
- 5.7 Ensure that, where communication tools such as email, chat and instant messaging are integrated into a service, the online presence or status matches the selected privacy setting. For example, if a profile is set to 'private', only accepted 'friends' or 'buddies' should be able to view the user's online presence or availability.
- 5.8 Consider screening or reviewing user profile photos, especially for users under the age of 18, using human and/or technical moderation, and removing inappropriate images or videos posted by users, but particularly if they are sexually provocative.
- 5.9 Have links in place, such as mechanisms to report abuse or flag profiles that may be inappropriate or that place the child or young person at risk.

6. SEARCH

Search applications can be powerful tools in 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 the age of 18.³⁵

RECOMMENDATIONS

Service providers should:

- 6.1 Take steps to ensure that private profiles of users under the age of 18 are not searchable (unless the user actively consents for their profile to be searchable), either on the service or via search engines.³⁶ This may be difficult for services that have already been developed around the legal age of consent, i.e. 16 years of age. However, future services should strongly consider using 18 years.
- 6.2 Social networking or interactive services with an integrated site search should not allow users to search public profiles of users under the age of 18 using sensitive personal data fields, such as age, sex and location, or school.

7. CONTENT SCREENING AND MODERATION

RECOMMENDATIONS

Service providers should:

- 7.1 Provide clear information (or Frequently Asked Questions – FAQs) on the various ways that users can reduce the risk of harassment or abuse. This information would include instructions on how to:
 - remove or block individuals;
 - prevent and remove the posting of anonymous comments; and
 - receive comments only from friends.

³⁵ <http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/search-and-advice-public.pdf>

³⁶ In the UK the age of consent is 16 and establishing contact with younger children (online or offline) in order to meet them at a later date for the purposes of engaging in sexual activity is an offence under section 15 of the Sexual Offences Act 2003.

- 7.2 Consider offering users an option to approve or pre-moderate comments which may be displayed on their individual site or to restrict the posting of comments only to ‘confirmed friends’. Ensure that this option is available for all aspects of the service (where technically feasible), for example for journals, blog entries, image galleries, videos and guest books.

- 7.3 Where site moderation is used, consider adopting the Home Office *Good Practice Guidance for the Moderation of Interactive Services for Children*.³⁷

8. IDENTITY AUTHENTICATION AND AGE VERIFICATION

In light of the current challenges concerned with identity authentication and age verification, service providers should continue to evaluate the effectiveness of technologies that identify and verify the age of customers. The goal should be to implement a suitable solution appropriate to their individual service, to the extent that the solution is legally and technically feasible, and most importantly creates a safer, more secure Internet environment for children and younger users.

DENYING ACCESS TO UNDER-AGE USERS

Service providers use a number of systems to deny access to users who declare that they are under 13 years of age. They also act against children who misrepresent their age to gain access to a service. For example, by:

- placing a ‘cookie’ onto a user’s computer to prevent the user from attempting to re-register with false age details;
- using technical tools such as search algorithms to look for words typically used by children and young people and identify children under 13 years old who may have lied about their age at registration; and

³⁷ <http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/moderation.pdf>

- offering free downloadable parental controls which help parents to manage their children's use of the service.

ADULT AND AGE-INAPPROPRIATE CONTENT

Some service providers allow users to post content with adult themes. It is important that, where this is permitted, service providers take reasonable steps to minimise the risk of children and young people from accessing this content.

RECOMMENDATIONS

Service providers should:

- 8.1 Make tools available which minimise the risk of users under the age of 18 accessing adult or other age-inappropriate content. Options may include:
 - allowing users to tag or label content as being 'adult' in nature or otherwise age-inappropriate;
 - providing labelling or tagging of users' content; and
 - technical means of protection, e.g. filtering.
- 8.2 Ensure that where specific services aimed at adults (e.g. sexual content, and dating or flirting sites) are offered, these areas are not accessible to users registered as under the age of 18.
- 8.3 Consider using available age-verification systems to verify that users accessing dedicated adult content or services, for example pornography or gambling, are aged 18 or over, such as:
 - a credit card check;³⁸
 - PIN numbers; and
 - proof of account ownership.

9. RESPONSIBLE USE AND MANAGING BULLYING AND OTHER FORMS OF ABUSE VIA COMMUNICATIONS TECHNOLOGY

Service providers employ various approaches to limit the ability of users to bully and harass other users, or to post content that breaches the terms and conditions of the service in other ways. As mentioned above, services often have features to enable users to protect themselves online. Some providers moderate services and others provide technical solutions to protect users of their service, or a combination of both.

A number of service providers have developed technical solutions that have shown promise in detecting and preventing bullying or misuse of their services, to the benefit of their users. For example, algorithms have been written that search for language indicative of threatening behaviour or for derogatory terms. However, these solutions are still in the early stages of development and they are not a panacea for all the safety challenges that users of social networking and interactive services face. And some sites have implemented blocking of individual users.

Some of the following recommendations appear under other sections in this guidance, but are repeated here because of their direct relevance to managing bullying via communications technology and encouraging responsible use.

RECOMMENDATIONS

Service providers should:

- 9.1 Give clear and prominent messages to users about:
 - the importance of behaving responsibly online;
 - their role in contributing to a positive and respectful community; and
 - the right of service providers to remove inappropriate content.

³⁸ Service providers should be aware that some pre-paid credit or payment cards are also used by people under the age of 18 and these may not be suitable for age verification.

9.2 Consider placement of relevant information within community guidelines, advice and help sections, and in prominent and appropriate locations throughout the site.

9.3 Inform users how to:

- block individuals entirely or remove people from their ‘friends’ list;
- use ‘ignore’ functions or similar tools;
- use moderation tools which allow users to pre-screen comments and limit other users’ access to specific content, e.g. photo album; and
- remove unwanted comments or content from their personal pages and, where possible, remove comments they have posted to other people’s pages.

9.4 Make users aware that their online activities are not anonymous and reports of bullying and harassment will be taken seriously. Users should be made aware that reports of abuse may result in action by the service provider, including termination of their account and that, in serious cases, the provider or a victim or their representative may initiate civil or criminal legal proceedings.

9.5 Ensure that the ‘report abuse’ system is easily accessible and easy to use, to report any bullying or abusive behaviour.

9.6 Enable visitors to social networking sites to report bullying and abuse, regardless of whether or not they are registered for the service. Information should be available on how to do this. For example, a dedicated email address could be supplied for making complaints to the service provider.

9.7 Encourage complainants to provide details to facilitate effective handling of the report by the provider. This may include:

- reason for complaint, e.g. threatening or abusive comments, fake profiles, inappropriate images, etc.;

- location of the content, e.g. URL of the webpage;
- type of content or communication, e.g. comment, photo or video, posting in blog;
- date the content was viewed or posted (where possible);
- screenshot/grab of the ‘offensive content’;
- encouraging mobile users to save any communications, including texts, multimedia messages or downloads and any associated mobile numbers or email addresses; and
- any other relevant additional information.

10. REPORTING CONCERNS, ABUSE AND ILLEGAL BEHAVIOUR

GENERAL

Service providers and law enforcement agencies have achieved a great deal of success in co-operating effectively to combat illegal activities online using well-established protocols and procedures. The emergence of national agencies, such as the Child Exploitation and Online Protection Centre (Appendix C) in the UK, and global bodies such as the Virtual Global Taskforce, offers scope to build on this co-operation.

Users of social networking services need to be able to access straightforward mechanisms to report matters that concern them. These matters could range from offensive communications or other behaviours, which breach providers’ terms and conditions, to potentially illegal activities, including but not limited to:³⁹

- posting images depicting child sexual abuse or exploitation;
- suspicious behaviour towards children and young people, including behaviour indicative of grooming;
- bullying and harassment;

³⁹ 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.

- posting of inappropriate content, such as information promoting or encouraging self-harm, suicide or eating disorders;
- incorrectly tagged adult or age-inappropriate content; and
- other potentially illegal or criminal behaviour.

It is for each service provider to make an assessment of how their services are used, which behaviours are likely to occur and how concerns can be addressed. Law enforcement can also have a role in advising providers how their services are being misused.

It is important to 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 helplines or support services. This would be particularly helpful in cases where victims of abuse or those with concerns may be reluctant to identify themselves or report directly to the service provider or law enforcement agency.

RECOMMENDATIONS

Service providers should:

- 10.1 Have in place clear and straightforward reporting mechanisms for users (in particular for children and young people) to report suspected abuse.
- 10.2 Consider placing relevant advice and links to these reporting options in prominent and relevant parts of the service where users are interacting with other users, such as instant messaging, chat areas, picture galleries, user profiles, message boards, guest book areas and blogs.
- 10.3 Continue to research, develop and test measures designed to detect suspicious behaviour towards children.
- 10.4 Consider establishing a general page with information and/or links where users can choose the appropriate agency or organisation to contact about making a report. This could include:
 - the service provider;
 - law enforcement agencies;
 - emergency services where there is an immediate threat to safety of life, or where a child or children are at immediate risk of harm, for example by phoning 999 (UK), 911(US) or 000 (Australia);
 - child welfare organisations such as the National Society for the Prevention of Cruelty to Children (NSPCC) or ChildLine; and
 - other confidential helplines/support services (e.g. hotlines⁴⁰ and support agencies).
- 10.5 Consider acknowledging each report received, confirming that it will be managed and an indication of the timescale, if appropriate.
- 10.6 Explore providing reporting mechanisms which automatically capture essential information and relevant evidence, such as a ‘screen capture’ of abusive, offensive or inappropriate content or communications, the online ID of the abuser and the date and time of the incident being reported.⁴¹

⁴⁰ Service providers should continue to report illegal images to the Internet Watch Foundation (UK), National Center for Missing & Exploited Children (NCMEC) (USA) or Australian Communications and Media Authority (Australia).

⁴¹ See previous Home Office Task Force on Child Protection on the Internet good practice models and guidance on chat services and instant messaging. www.homeoffice.gov.uk/documents/ho_model.pdf

- 10.7 It is essential that users, particularly children and young people, of social networking and user interactive services are able to report to law enforcement agencies in a way that is user friendly and with minimum delay. In the UK, users should be able to report directly⁴² to the Child Exploitation and Online Protection Centre (CEOP)/Virtual Global Taskforce (VGT) (e.g. via report abuse button or hyperlink) for matters concerning suspected, attempted or actual online sexual abuse, including grooming.
- 10.8 It is recognised that some media platforms (e.g. mobile or PDA devices) currently have limitations that may make some direct reporting solutions difficult. It is important to keep developments under review.

11. RELATIONSHIPS BETWEEN SERVICE PROVIDERS AND LAW ENFORCEMENT

RECOMMENDATIONS

Service providers and law enforcement should:

- 11.1 Consistent with applicable laws, make arrangements to share reports of potentially illegal incidents and suspicious behaviour relating to the protection of children. These arrangements, depending on local jurisdiction and applicable laws, may include:
- guidelines or protocols on what content and supporting information service providers should preserve as evidence;
 - protocols for disclosure which are compliant with relevant data protection and privacy legislation; and
 - feedback mechanisms between industry and law enforcement agencies.
- 11.2 Continue to research, develop and test ways of detecting potentially illegal and/or suspicious behaviour towards children online.

⁴² Service providers wishing to facilitate or adopt direct reporting are encouraged to seek the advice of CEOP or their local VGT partner (Online Child Sex Exploitation Team (OCSET) in Australia/NCMEC in USA) on potential options.

PART 3

Safety tips



These safety messages are for parents, carers, children, young people and service providers. The safety tips draw on the available research, and issues discussed in the Home Office Task Force project group.

The information in this section is intended to help provide material for any media literacy, education, awareness or campaign work that providers or others may wish to develop.

1. SAFETY TIPS FOR PARENTS AND CARERS

BECOME FAMILIAR WITH SOCIAL NETWORKING AND USER INTERACTIVE SITES

- You should not be afraid to become involved in your children's online activities. Most social networking and user interactive sites are easy to examine and evaluate, and children are best protected when they communicate with their parents or carers.
- Ask your child about what social networking and user interactive sites they use and how they work. This will help you understand your child's interests and enable you to assess how well they understand the issues associated with using the service.
- Depending on the age of your child, consider the use of parental controls such as filtering or monitoring software on which you can set the permissions to manage your child's access to social networking sites. For more information on such tools, see www.getnetwise.org.
- It is important to remember that social networking and interactive sites can be accessed through a mobile device as well as a PC or laptop. So any discussions with your child should cover how they access and use social networking sites, including, for example, through their mobile phone.
- You should become familiar with the social networking and interactive sites your children are using. Pay particular attention to:
 - i the terms and conditions of the site (i.e. the rules for using the service), but particularly to what is acceptable behaviour or not on the service.
 - ii the age requirement to register for the service, for example whether the service is suitable only for children 13 years and over;
 - iii the safety advice that is provided on the service for the user; and
 - iv the safety tools on the service, including:
 - user profiles – view user profiles to check what personal information is published;
 - privacy controls – look for privacy tools offered by a site, what the privacy settings are (e.g. whether private or public for those under the age of 18 years) and how they can be changed; and
 - reporting concerns – check how users can contact or report any difficulties they are having to the service provider or other agencies.
- Teach children the importance of registering their correct age to ensure that the safety protection tools provided for those under the age of 18 are applied to them so they get the most appropriate content and experience.
- Visit the sites and familiarise yourself with the features the sites have on offer, such as creating a webspace, creating a profile, blogging, making friends, instant messaging and chatting, posting videos and photos.
- Remind your child to review their contact/friends list on a regular basis to make sure they want to share their information with everyone on the list.
- Negotiate with your child to visit and view all their profiles on social networking sites; some children have a version for their parents and another for their friends.
- Discuss with your child the mechanisms available to them to manage their profile. All

users can change their privacy settings, block users and report abuse, and have the option to cancel their account.

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, while respecting their privacy.
- 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.

GUARDING PRIVACY

- It is critical that children and young people understand the importance of protecting their privacy online. Many, if not all, of the popular social networking sites provide privacy tools to ensure that users can manage whom they choose to interact with and who can post the comments on their blogs or personal sites.
- It is important that children and young people think carefully about adding someone they have only met online 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 account or space private to protect against someone taking control of it.
- Mobile phones can be easily lost or stolen. It is a good idea to set up a PIN lock on your child's mobile, so it cannot be used without their permission or if it is lost or stolen.
- Your child should only use auto login (where the site remembers your password for you when you return to it) when signing into a social networking site if PIN protection is being used on their mobile. Otherwise anyone finding their

mobile phone and accessing the site from it will be able to access and abuse their social network account, for example by changing their profile, or sending messages to contacts in their name.

- 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 to be careful not to share any information that may help locate them in the real world. For example, a photograph of a school uniform or street sign.

MANAGING PERSONAL IMAGES AND VIDEO POSTINGS

The use and sharing of images and videos has proliferated online, especially on social networking and video-sharing sites. Images and videos can be loaded from cameras and mobile phones. Some mobile devices enable users to upload images and videos directly to social networking 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.
- The convenience of mobile phones means it is easy to upload images and videos 'on the go'. Particular care should be taken to 'think before you post' to avoid compromising privacy or safety, for example images from a party or of outrageous or compromising behaviour. If a child is posting photos containing their friends, for example, they should seek their friends' permission first.
- Photos and videos can contain information that on its own may seem innocuous, but when put together with other information such as school details can be used to locate and identify the child.

- Photos and videos should be appropriate – not sexually provocative or explicit – 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 user interactive sites. Most sites will remove explicit and ‘inappropriate’ images when they are brought to their attention.
- Ask 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.

MANAGING COMMENTS AND POSTINGS

Many young people go to great lengths in building their profiles and webpages, 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 among known friends or peers on social networking sites – where bullying in the playground has continued and possibly escalated online. The potential to humiliate and harass individuals through comments and by 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 to set rules with your child about what is OK and 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 take it back. It is also important to be aware that what may be sent or posted as a joke, may not be taken in that way. When a message is posted to or about someone, the sender cannot see the impact that their words or images have on the other person.

MANAGING YOUR TEENAGER’S FLIRTATIOUS BEHAVIOUR

- It is important to discuss and establish boundaries with your child from an early age, about flirting online, especially when your child begins to show an interest in and is beginning to use interactive services.
- Teenagers 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.
- You should discuss, and emphasise, particularly with older teenagers, the dangers of flirting with people they have first met online. As some people lie about who they are, you never really know who you are interacting with or talking to.

MEETING IN PERSON WITH PEOPLE FIRST MET ONLINE

Meeting people in the real world who are only known online 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, 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 that any such meetings should be approved by their parents or carers.
- You should ensure that any meetings take place in public and with trusted adults present.
- It is important to address and consider the possibility of your child being involved in organised ‘gang’ or rivalry meetings in the real world, which can be arranged online.
- It is also important to recognise that there are online groups and communities where children and young people meet that can be educational and fun.

GETTING HELP AND REPORTING ABUSE

- It is critical to maintain an ongoing dialogue and have regular conversations with your child 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.
- Preserving the evidence of any abusive or potentially illegal communication is important. This evidence can be helpful if you need to report to the child’s school, the service provider or to the police. If you have any copies of communications, images, messages or other content related to the solicitation of a child, it is important to save them and pass them to law enforcement agencies.
- It is very important that both you and your child understand 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 potentially illegal behaviour online, for example:
 - i in the UK, the Child Exploitation and Online Protection Centre (CEOP) (www.ceop.org.uk), see Appendix C for more information about CEOP; and
 - ii in the US, the National Center for Missing & Exploited Children (NCMEC) CyberTipline (www.cybertipline.com), see Appendix G for more information about NCMEC and the CyberTipline.

2. SAFETY TIPS FOR CHILDREN AND YOUNG PEOPLE

Many children and young people have an online profile 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. However, as in the real world, it is important that you take care of yourself, your friends and the wider community.

The following tips will be useful whether you access your social networking site through a PC, laptop, games console or mobile phone.

STAY IN CONTROL – GUARD YOUR PRIVACY

Social networking sites are used mostly to connect with friends you know in the real world. So you might not think about strangers getting hold of your personal information, such as your mobile number, email address or where you live. But it is important to think about the information you post on your page and on other people’s.

- Before setting up your profile, think about who you want to see your personal information.
- Different social networking sites have different privacy settings – read about these carefully and decide who you want to see your personal information.
- If you only want people you know to see information about you – set your profile to private. This is the recommended option.
- Every now and again, look through your contacts or friends and make sure you still want them to know your personal details. Remember, it’s not how many people you know but how well you know them.
- ‘Private mode’ may be safer than ‘public mode’, but arguments can still occur between friends. People you know could use something you have posted against you, for example to bully you or to damage your reputation. Think very carefully about what you share with your friends.

- It is important to protect your password – don't give it to your friends even for fun. If you give it to them, you just cannot be sure who they might pass it on to.
- If you use your mobile on social networking sites, remember mobile phones can be easily lost or stolen and you don't know who could get your information, or pretend to be you. Put a PIN lock on your mobile, so it can't be used without your permission.
- If your computer or mobile remembers your password, use a PIN number or password every time you sign in.
- Make sure that you register your real age so that other people don't think you are older than you are and treat you in a way that is inappropriate.

'GOING PUBLIC'

If you intend to share your profile and content with everyone who is online, there are several things to think about.

- Are you sure you want to do this? You won't be in control of who will see your information.
- Be cautious – 'going public' may lead to things you didn't mean to happen. Be careful about the kind of information (including images) you share about yourself and how you manage your online reputation. Other people can pass on or change your information and you might not be able to stop them or delete it afterwards.
- Remember, when you 'go public', it is not just 'friends of friends of friends' but also complete strangers who will be able to see your content, search and find you online.
- Some social networking sites have a range of settings between public and private – select the one that is appropriate for you.

'UPLOADING CONTENT'

One of the best things about social networking is that you can 'upload' your content online – including images, videos and music that you have created yourself. This can be a lot of fun. But again, there are some things to think about before you do this.

- Remember, the World Wide Web is available to everyone, and if your profile is public, everyone can see everything you post about yourself and your friends.
- Be aware of how your content could be used or misused by others. For example, pictures can be copied, or altered and posted elsewhere. You may not even know this has happened. And if you do find out about it, you may not be able to stop it or remove it.

Guard your online reputation

- Information you post will reflect the kind of person you are, and it will influence what others think of you. What is your content saying about you?
- Think carefully before uploading content and sharing information that shows you or your friends in a compromising situation – for example images of friends drinking at a party.
- Don't post images of yourself posing in a sexual or provocative way. These can cause you a lot of embarrassment or upset if misused by others in a way you didn't anticipate, and could attract a lot of unwanted and unwelcome inappropriate contact.
- Also, ask your friends first, if they are identified in the content. Protect your friends and family: they have reputations too!
- It is important to understand that **you are not anonymous online**. You can be traced even if you gave a fake email account and registration information. Every computer and device connected to the Internet has a unique address

(given by your Internet service provider). This is linked to your computer in the real world – to your real-world address. The police, and some others, can access this address, and it is linked to every communication you send online.

Consider your friends

- Remember that what may seem funny to you can actually be very hurtful and offensive to others – so ‘think before you post’ comments on other people’s webspaces.
- You know how easy it is to upload images and videos ‘on the go’ using your mobile. Think carefully before you post so you don’t embarrass yourself or your friends.
- Don’t post content that may be seen as racist, homophobic, bullying or threatening. Remember, these sorts of behaviours could result in your account being deleted by your service provider, and the police may even get involved.
- Try not to bring disagreements or arguments with people that you know in real life into the online community.
- Setting up a fake page to pose as someone else may seem a clever way to embarrass the person you are impersonating. But this can have very serious consequences – to the other person and, in fact, to yourself, as the police may become involved.
- Remember to be a good friend and, if your friends are behaving inappropriately, remind them that they are not anonymous and can be traced.

Copyright – get permission

- Copyright is the protection given to authors (of writing, images, video or music). It protects them from other people copying their work without permission. It is important to respect this.

- If you download or copy something from the Internet without permission, there can be serious consequences, including from the police.
- You can use a Creative Commons licence to make your own creative work freely available to others. For example, you can change your copyright terms from ‘all rights reserved’ to ‘some rights reserved’. See <http://creativecommons.org>.

RESPECT THE ONLINE COMMUNITY

People online love interactions that are interesting, funny and witty; this contributes to making the Internet entertaining for everyone. There are also some ways to show your respect for other people online.

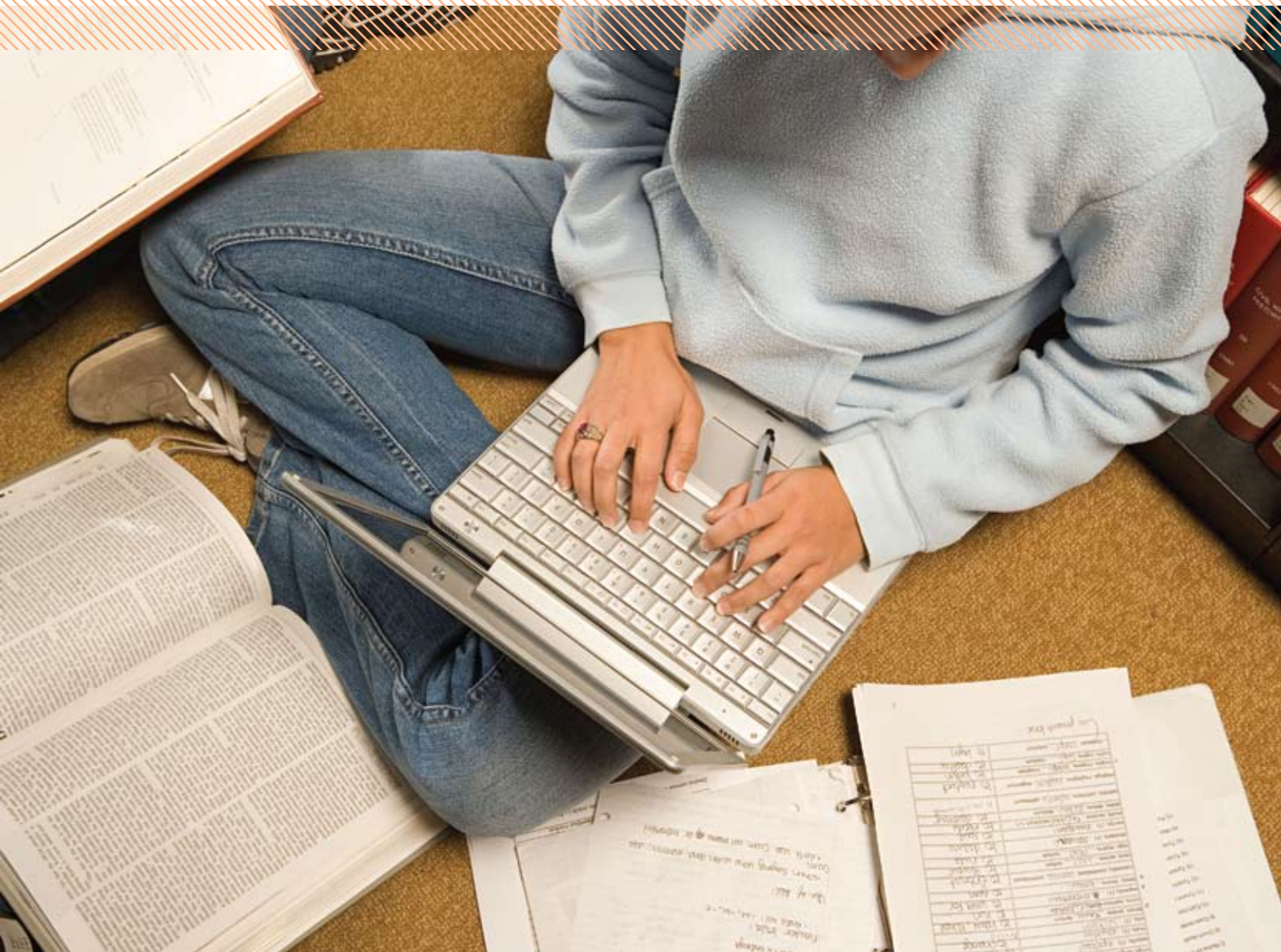
- Respect what other people contribute and the time and effort they have put into creating and sharing content.
- The Internet is a very public place, so personal disagreements can quickly get out of control. This may result in public humiliation, hurt or distress beyond what you ever intended.
- If you realise that someone else is having problems – for example receiving threats, bullying or nasty behaviours – try not to make things worse. Report the situation to your service provider and seek their help and advice. They should respond to you.

JUST DON’T TAKE IT! – REPORTING ABUSE AND SEEKING ADVICE AND HELP

- If problems or difficulties happen on the Internet, use the tools provided on the service to block, ignore, filter or report these to your service provider, for example the social networking provider.
- You will find contact information from your social networking provider. They should have links to sources of expert help and advice on pages titled ‘Help’, ‘Customer care’ or ‘Report abuse’.

- Remember, arranging to meet someone that you have only met online is dangerous, and it is safer not to do so. Only do so with your parent's or carer's permission, take a trusted adult with you, and meet in a public place.
- If someone else's behaviour online makes you feel that you or someone else is in immediate danger, you should act urgently and contact the police.
- There are now a number of places to report potential illegal behaviour online, particularly if someone approaches you in a sexual way:
 - i in the UK, the Child Exploitation Online Protection Centre (CEOP) – www.ceop.org.uk; and
 - ii in the US, the National Center for Missing & Exploited Children (NCMEC) CyberTipline – www.cybertipline.com.
- Speak to an adult or friend that you trust if you are unsure about anything. It is always good to seek advice or help if anything makes you feel scared or uncomfortable.

Appendices



APPENDIX A: THE CRIMINAL LAW

THE CRIMINAL LAW AFFECTING PERSONAL INTERACTIONS IN INTERACTIVE SERVICES

It is important to note the general principle that an action that is illegal if committed offline is also illegal if it is committed online. This applies both to issues such as distributing illegal material and also to harmful behaviour if it amounts to a course of harassment, or grooming. Inciting someone to commit an offence is no less an offence simply because it is done through a computer or mobile phone. Other criminal activity may include fraud and identity theft. Each case will be different, and it is impossible to set out in a document of this sort a definitive explanation of the law. Nevertheless, it is hoped that this brief and general guide to a few relevant offences, particularly those involving children, will be helpful. No-one using an interactive service should be under the illusion that the criminal law does not bear on what they do. Some of the legislation below applies only to England and Wales, although Scotland, Northern Ireland and other jurisdictions such as the United States (see also Appendix G) will have equivalent legislation.

PROTECTION FROM HARASSMENT ACT 1997

The Protection from Harassment Act 1997 extends to any form of persistent conduct which causes another alarm or distress. Section 4 of the Act makes it a criminal offence for a person to pursue a course of conduct which he knows, or ought to know, will cause another to fear violence. This offence will catch the most serious cases where behaviour is so threatening that victims fear for their safety. It carries a penalty of a maximum of five years' imprisonment and/or an unlimited fine.

Section 2 of the Act provides for a further offence in cases of a course of conduct which the perpetrator knows, or ought to know, will cause harassment. This offence will catch the sort of persistent conduct which, although it may not make the victim fear that violence will be used, nonetheless can have devastating effects.

It carries a penalty of a maximum of six months' imprisonment and/or a level five fine. A court sentencing someone convicted of an offence under either of these sections may also impose a restraining order prohibiting specified forms of behaviour. Breach of a restraining order is a criminal offence punishable by up to five years' imprisonment.

In addition to these criminal offences, section 3 of the Act provides a civil remedy which enables a victim to seek an injunction against a person who is harassing them or may be likely to do so.

PROTECTION OF CHILDREN ACT 1978

The Protection of Children Act 1978 essentially prohibits the creation or distribution of indecent photographs of children. Proscribed activities are taking, making, permitting to be taken or made, distribution or showing, possessing with intent to possess or show, or publishing an advertisement for such photographs. The maximum penalty is ten years' imprisonment. Simple possession of an indecent photograph is an offence under section 160 of the Criminal Justice Act 1988, and carries a maximum penalty of five years' imprisonment. Although there are defences specified in the Acts, it is unlikely that any of these could apply to images that might be sent over a public interactive service, so anything discovered in a service that appears to be an indecent photograph of a child needs to be reported and properly investigated.

SEXUAL OFFENCES ACT 2003

Section 10: Causing or inciting a child to engage in sexual activity

Section 10 makes it an offence for a person to cause or incite a child to engage in sexual activity. This encapsulates all sorts of sexual behaviour, including when a person is seeking to get a child to perform a sex act on itself. For example, if A asks B (a child) to touch herself or to pose in her underwear before a webcam, it is quite possible that a jury may consider this to be a sexual act. What amounts to a 'sexual' activity will be decided

by the court, but section 78 of the Act defines 'sexual' in such a way that the circumstances and motives of an offender may be relevant. The offence is committed even where the child apparently consents to performing the act.

The offence has a maximum penalty of 14 years' imprisonment.

Section 12: Causing a child to watch a sexual act

Section 12 makes it an offence for a person aged 18 or over to intentionally cause a child aged under 16, for the purposes of his own sexual gratification, to watch a third person engaging in sexual activity, or to look at an image of a person engaging in a sexual act. The act can be live or recorded, and there is no need for the child to be in close physical proximity to the sexual act. Examples of this offence would be where a person, for the purposes of his own sexual gratification, enables a child to watch two people have sex, either in the physical presence of the activity or remotely, for instance via a webcam; or where someone invites a child to watch a pornographic film.

The offence does not require any element of coercion, though it may be a factor in some cases. The offence is committed even where the child apparently consents to watching a sexual act. In order for an offence to be committed, the adult must act for his own sexual gratification. The offence has a maximum penalty of ten years' imprisonment.

Section 15: Meeting a child following sexual 'grooming'

Section 15 makes it an offence for a person aged 18 or over to meet intentionally, or to travel with the intention of meeting, a child under the age of 16 in any part of the world, if he has met or communicated with that child on at least two prior occasions, and intends to commit a 'relevant offence' against that child either at the time of the meeting or on a subsequent occasion.

The section is intended to cover situations where an adult establishes contact with a child and gains the child's trust so that he can arrange to meet the child for the purpose of committing a 'relevant offence' against the child (essentially this means sex offences). The contact with the child may take place through communications on the Internet, but equally it could, for example, be through meetings, letters, text messages or telephone conversations. The police may become aware of the contact between the offender and the child by a number of means, for example reporting by the child, or by concerned parents/teachers.

An offence is not committed if the adult reasonably believes the child to be 16 or over. In cases where the defendant claims to have reasonably believed that the child was 16 or over, it is for the prosecution to prove that he held no such belief or that his belief was not reasonably held.

The initial communications between the adult and child may have a sexually explicit content, for example conversations about sexual acts he would like the child to engage in or sending the child indecent images. However, this need not be the case. Prior communications could, for example, involve an adult giving a child music lessons or running a youth club the child attends, an adult serving sweets to a child in a sweet shop, meeting incidentally through a friend, or chatting about innocent subjects. It is for prosecutors to prove the intent of the adult to engage in unlawful sexual behaviour with the child on the occasion of the meeting or on a subsequent occasion. Such evidence might be obtained by examining the contents of emails or letters which have been sent or received, or from the transcripts of chat room conversations which might have been logged either on an individual's computer or on the computer of an Internet service provider. Evidence may also be drawn from other circumstances.

The intended 'relevant offence' does not have to take place for the offence to be committed. It is sufficient for the adult to travel to meet the child with the intent to commit a 'relevant offence' against the child.

Either the meeting or at least part of the travel to the meeting must take place in England, Wales or Northern Ireland. However, the adult's previous meetings or communications with the child can have taken place anywhere in the world, and it would also be possible for the person to intend to engage in sexual activity with a child in another jurisdiction.

In some cases it might be appropriate to charge a person with an attempt to commit the offence rather than the offence itself. For example, where an undercover policeman takes the place of the child at the meeting in a covert operation, the defendant could be charged with attempting to commit the offence, assuming the necessary intent could be proved. The attempted offence has the same penalty as the offence itself. The offence has a maximum penalty of ten years' imprisonment.

COMMUNICATIONS ACT 2003

Section 127 (1) provides that it is an offence if any person sends a message or other matter by means of a public electronic communications network that is grossly offensive, indecent, obscene or menacing, or if a person causes any such message or matter to be sent.

Section 127 (2) provides that a person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he sends or causes to be sent by means of a public electronic communications network a message he knows to be false, causes such a message to be sent, or persistently makes use of a public electronic communications network.

The offences carry a penalty of a maximum of six months' imprisonment and/or a level five fine (£5,000).

Appendices B–H have been contributed by the individual organisations and authors. They are intended to complement this guidance and offer relevant information about issues related to the guidance.

The contents may reflect the opinions and views of the organisations, not those of the Home Office or the Social Networking and User Interactive Services Project Group.

APPENDIX B: CHILDREN AND THE INTERNET

Sonia Livingstone (Professor of Social Psychology, London School of Economics and Political Science)

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 teenagers 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 UK Children Go Online (UKCGO) study¹ 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 years) 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 old daily and weekly users have received unwanted sexual (31%) or nasty (33%) comments 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 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 teenagers 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.²

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 have sent a photograph (7%) to someone that they met on the Internet.

Many children are aware of the risks, but the outcome (for themselves and their parents/teachers) is to increase rules, restrict access and reduce their participation online, and so reduce the benefits they could gain from the Internet.

¹ See www.children-go-online.net.

² 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 one in three 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. and McFarlane, L. (2003), Online harassment: Towards a definition of cyberstalking. *Prison Service Journal*, 139, 31–38. See also Millwood Hargrave, A. and Livingstone, S. (2006), *Harm and Offence in Media Content: A review of the evidence*. Bristol: Intellect.

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 by research to be effective.³

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.⁴ 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 what 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 people's Internet use, particularly now social networking has become commonplace.

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.'⁵

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.⁶ 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).

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 well as offline.

³ Livingstone, S., Bober, M. and Helsper, E. J. (2005), *Internet literacy among children and young people*. London: LSE Report, February 2005. www.children-go-online.net and <http://personal.lse.ac.uk/bober/UKCGOonline-literacy.pdf>

⁴ Livingstone, S. (2006), Children's privacy online. In R. Kraut, M. Brynin and S. Kiesler (Eds), *Computers, Phones, and the Internet: Domesticating Information Technologies* (pp. 145–167). New York: Oxford University Press.

⁵ Lorie, 17, from Essex, interviewed by the UKCGO project.

⁶ 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 are 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.

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.

Brown⁷ 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.⁸

The authors contributing to Mazzarella's volume, *Girl Wide Web*,⁹ 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.'

Stern's¹⁰ analysis of teenage girls' homepages 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 that society may fail to provide a sufficiently rich environment for them. Clearly, a balance between these two positions would be appropriate.

⁷ Brown, J. D., Halpern, C. T. and L'Engle, K. L. (2005), Mass media as a sexual super peer for early maturing girls. *Journal of Adolescent Health*, 36(5), 420–427.

⁸ Buckingham, D. and 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.

⁹ Mazzarella, S. R. (Ed.) (2005), *Girl Wide Web: Girls, the Internet, and the negotiation of identity*. New York: Peter Lang.

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 and K. Walsh-Childers (Eds), *Sexual Teens, Sexual Media: Investigating Media's Influence on Adolescent Sexuality* (pp. 265–285). Mahwah, NJ: Lawrence Erlbaum Associates.

Cooper, a paediatrician, argues that teenagers' brains do not reach physical and cognitive maturity until the age of nearly 21 years,¹¹ 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.¹² The influence of the peer group grows in importance during adolescence as the influence of parents declines (though remains substantial).

Coleman and Hendry¹³ 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 teenagers 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' (pp.92–93).

¹¹ See www.netsmartz.org/safety/.

¹² A fair summary of child development is provided in the table on pp.116–17 in Thornburgh, D. and 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 Coleman, J. and Hendry, L. (1999), *The Nature of Adolescence* (third edn). London: Routledge.

WHAT'S NORMAL, WHO IS VULNERABLE?¹⁴

The National Center for Missing & Exploited Children (aged 10–17 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 with 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 with youths with mild/no symptoms.¹⁵ 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 youths, including many commonalities with aggressor-only youths, 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.¹⁶

¹⁴ See Millwood Hargrave, A. and Livingstone, S. (2006), *Harm and Offence in Media Content: A review of the evidence*. Bristol: Intellect.

¹⁵ Ybarra, M. L., Leaf, P. J. and Diener-West, M. (2004), Sex differences in youth-reported depressive symptomatology and unwanted Internet sexual solicitation. *Journal of Medical Internet Research*, 6(1).

¹⁶ Ybarra, M. L. and 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. and 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.

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.¹⁷ 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 teenagers 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, victimisation) and gay-related stressors, particularly those directly related to visible and behavioural 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.¹⁸

Sonia Livingstone, December 2006

¹⁷ Beebe, T. J., Asche, S. E., Harrison, P. A. and 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.

¹⁸ Savin-Williams, R. C. and Ream, G. L. (2003), Suicide attempts among sexual-minority male youth. *Journal of Clinical Child and Adolescent Psychology*, 32(4), 509.

APPENDIX C: CHILD EXPLOITATION AND ONLINE PROTECTION CENTRE (CEOP)

WHAT IS CEOP AND WHAT DOES IT DO?

CEOP has the legal remit and authority for tackling child sexual exploitation within the UK including the online environment, 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 exploitation.

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 or exploited by an adult or is at potential risk of such. 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.

CEOP 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.co.uk.

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, uncovers suspicious behaviour/communications that may suggest online child sexual abuse; and
- 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. For that reason, in cases of online child sexual exploitation involving suspected, attempted or actual online child sexual abuse, it is essential that users, particularly children and young people, are able to report directly to law enforcement with minimum delay from the online environments they frequent and where the threats manifest themselves. This should be achieved through direct reporting to CEOP in the UK and best achieved through the adoption of the CEOP/VGT ‘Report Abuse’ mechanism by online providers, whose services are aimed at or are very likely to attract children and young people.

It is CEOP’s experience that this works best by placing the mechanism in a prominent position within the online spaces that children and young people occupy. Therefore, it is important that online providers who adopt the CEOP/VGT ‘Report Abuse’ mechanism seek the advice of CEOP or the relevant VGT partner when implementing the mechanism, to ensure that it is placed in prominent areas so as to facilitate enhanced safeguarding for children and young people and deterrence from future offending.

The CEOP/VGT 'Report Abuse' mechanism allows the public to report their concerns directly to CEOP in the UK, the National Center for Missing & Exploited Children (NCMEC) in the US, AFP/OCSET in Australia, RCMP, NCECC in Canada, Postal and Communication Police in Italy and Interpol for the rest of the world.

It is recognised that the scope for embedding the mechanism within some environments, for example mobile phones, may be limited at this current time. However, as technology/associated services develop in these areas, or where the threats to the safety of children and young people are identified, the provider or operator should work with CEOP or the relevant VGT partner to ensure that the "Report Abuse" mechanism is considered as part the development process.

For further information on the CEOP/VGT 'Report Abuse' mechanism, please go to www.ceop.gov.uk.

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 2007/08 a bespoke system for industry to report concerns directly to CEOP is planned.

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 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 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 are 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 National Society for the Prevention of Cruelty to Children (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. 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 an adult, and Childline or the 'There4me' website (www.there4me.com), if a child or young person.

APPENDIX D: INTERNET WATCH FOUNDATION (IWF)

WHAT IS THE IWF AND WHAT DOES IT DO?

The IWF (www.iwf.org.uk) is the only recognised non-statutory organisation in the UK operating an Internet ‘hotline’ for the public and IT professionals to report their exposure to potentially illegal content online.

Its aim is to minimise the availability of potentially illegal Internet content, specifically:

- child sexual abuse images hosted anywhere in the world;
- criminally obscene content hosted in the UK; and
- incitement to racial hatred content hosted in the UK.

The IWF works in partnership with UK government departments such as the Home Office and the Department for Business, Enterprise and Regulatory Reform to influence initiatives and programmes developed to combat online abuse. This dialogue goes beyond the UK and Europe to ensure greater awareness of global issues and responsibilities.

It is funded by the EU and the online industry. This includes Internet service providers, mobile operators and manufacturers, content service providers, telecommunications and filtering companies, search providers and the financial sector, as well as blue-chip and other organisations who support the IWF for corporate social responsibility reasons.

Through the ‘hotline’ reporting system, IWF helps all service providers in the UK to combat abuse of their services through a ‘notice and take-down’ service by alerting them to any potentially illegal content within their remit on their systems and simultaneously inviting the police to investigate the publisher. As a result, less than 1% of potentially illegal content is apparently hosted in the UK, down from 18% in 1997. The IWF works closely

with CEOP and is a member of INHOPE (Association of Internet Hotline Providers: www.inhope.org).

As the number of people using the Internet and the diversity of content available continues to grow, the mechanisms for dealing with illegal content must be better known and understood. In partnership with many organisations, they strive to create continued awareness of the role and purpose of the IWF and aim to foster trust and reassurance in the Internet for current and future users.

APPENDIX E: NSPCC AND CHILDLINE

The National Society for the Prevention of Cruelty to Children's (NSPCC's) purpose is to end cruelty to children. The NSPCC has 177 community-based projects and runs the Child Protection Helpline and ChildLine in the UK and the Channel Islands. Most of the NSPCC's work is with children, young people and their families. However, the NSPCC also works to achieve cultural, social and political change – influencing legislation, policy, practice, public attitudes and behaviours.

The NSPCC wants to see a society where all children are loved, valued and able to fulfil their potential. To do this, it has four objectives:

- to mobilise everyone to take action to end child cruelty;
- to give children the help, support and environment they need to stay safe from cruelty;
- to find ways of working with communities to keep children safe from cruelty; and
- to be, and be seen as, someone to turn to for children and young people.

SERVICES REFERENCED IN THIS GUIDANCE PROVIDING INFORMATION AND SUPPORT

ChildLine (0800 111)

In February 2006, ChildLine and the NSPCC joined forces to help, support and protect even more children and young people. It was a natural fit, with both charities aiming to be someone for children and young people to turn to in times of danger or distress.

ChildLine is the UK's free, 24-hour helpline for children in distress or danger. Trained volunteer counsellors comfort, advise and protect children and young people who may feel they have nowhere else to turn. Over 1,000 volunteers provide a counselling service, supervised by a team of professional supervisors and managers. Most children who call ChildLine once talk with a counsellor about a problem or an issue they are struggling with, and then hang up knowing they can call again.

The NSPCC Child Protection Helpline (0808 800 5000)

The NSPCC wants to make sure that adults concerned about the welfare of children and young people have someone to turn to about their concerns. The NSPCC Child Protection Helpline is the only free and anonymous way for the public to take action to protect a child. The service provides:

- free telephone and email access to trained child protection staff 24 hours a day, 365 days a year;
- specialised support, advice, counselling and information for anyone who has concerns about a child at risk of abuse or who is being abused; and
- diverse, accessible services reaching out to protect all young people, especially those who need it most.

The NSPCC Helpline also incorporates the following other methods which enable it to reach as many adults as possible:

- Asian Language Helpline – direct: 0800 096 7719;
- email: Helpline@nspcc.org.uk; and
- textphone service for deaf and hearing-impaired callers – direct: 0808 100 1033.

APPENDIX F: SAMARITANS/ BEFRIENDERS WORLDWIDE

Samaritans is the lead organisation in the UK providing support for those experiencing feelings of distress or despair, including those which may lead to suicide. Its mission is to be available 24 hours a day to provide confidential emotional support for people. This takes place in a context that recognises the importance of having the opportunity to explore difficult feelings, based on the acceptance that everyone has the right to make fundamental decisions about their own life.

Samaritans has its own web presence at www.samaritans.org (and internationally through Befrienders Worldwide at: www.befrienders.org) and aims to make this the primary website for people interested in, concerned about or actively considering suicide or self-harm.

Support by email is provided as a fully integrated service within Samaritans and all messages are treated with equal respect and consideration as a telephone call, letters, or face-to-face sessions. Operating the service this way allows people to explore difficult issues in confidence and without any burden or guilt or responsibility being placed on them. Anecdotal feedback from the service suggests it is used by some people to help them organise their thoughts prior to contacting other agencies. To maintain the anonymous and confidential nature of the service, Samaritans uses bespoke email software and a secure server to remove all identifiers from received emails. Replies are then matched back to the contact details (via the server).

Samaritans is working with the Internet industry to develop systems allowing Internet and search engine providers to promote Samaritans when users search for information related to suicide or self-harm. For example, if 'I want to kill myself' is typed into most of the popular search engines, the results page should promote Samaritans (and Befrienders Worldwide) above all other sites.

From here, links can be made to the email support service or to Samaritans' international network partners IFOTES and Lifeline International.

With the development of social networking, Samaritans has developed a series of tools and interventions, including auto-responders for non-moderated forums, that can be used by these organisations to signpost to Samaritans, along with training for moderators to help them understand and work with people displaying behaviours that may be of concern (www.samaritans.org/training).

Postings on social networking sites relating to suicide and self-harm are opportunities for Samaritans to engage with the user, so Samaritans does not request these postings to be removed but instead advises promoting contact to Samaritans.

Samaritans aims to ensure that a variety of methods to contact the service are promoted across all media. Campaigns promote the phone number 08457 90 90 90 (1850 60 90 90 in Republic of Ireland), website www.samaritans.org and email jo@samaritans.org because multi-function devices such as the iPhone now allow both passive and active contact with Samaritans.

Anthony Langan – Samaritans, Public Affairs Manager

APPENDIX G: NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (NCMEC) AND THE CYBERTIPLINE

WHAT IS NCMEC AND WHAT DOES IT DO?

The National Center for Missing & Exploited Children's® (NCMEC) mission is to help prevent child abduction and sexual exploitation; help find missing children; and assist victims of child abduction and sexual exploitation, their families, and the professionals who serve them.

NCMEC was established in 1984 as a private, nonprofit 501(c)(3) organization to provide services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. Pursuant to its mission and its congressional mandates (*see* 42 U.S.C. §§ 5771 *et seq.*; 42 U.S.C. § 11606; 22 C.F.R. § 94.6), NCMEC:

- Serves as a clearinghouse of information about missing and exploited children
- Operates a CyberTipline that the public may use to report Internet-related child sexual exploitation
- Provides technical assistance to individuals and law-enforcement agencies in the prevention, investigation, prosecution, and treatment of cases involving missing and exploited children
- Assists the US Department of State in certain cases of international child abduction in accordance with the Hague Convention on the Civil Aspects of International Child Abduction
- Offers training programs to law-enforcement and social-service professionals
- Distributes photographs and descriptions of missing children worldwide
- Coordinates child-protection efforts with the private sector
- Networks with nonprofit service providers and state clearinghouses about missing-persons cases
- Provides information about effective state legislation to help ensure the protection of children.

The Congressionally mandated CyberTipline is a reporting mechanism for cases of child sexual exploitation including child pornography, online enticement of children for sex acts, molestation of children outside the family, sex tourism of children, child victims of prostitution, and unsolicited obscene material sent to a child. Reports may be made 24 hours per day, 7 days per week online at www.cybertipline.com or by calling 1-800-843-5678.

WHAT TYPE OF REPORTS DOES THE CYBERTIPLINE HANDLE?

Possession, Manufacture, and Distribution of Child Pornography

Child pornography has been defined under federal statute as a visual depiction of a minor (child younger than 18) engaged in sexually explicit conduct (18 U.S.C. 2256).

Online Enticement of Children for Sexual Acts

Use of the Internet to entice, invite, or persuade a child to meet for sexual acts, or to help arrange such a meeting, is a serious offense (18 U.S.C. 2425).

Prostitution of Children

Prostitution is generally defined as performing, offering, or agreeing to perform a sexual act for any money, property, token, object, article, or anything of value (18 U.S.C. 2431, 2423(a)).

Sex Tourism Involving Children

It is against the law for any United States citizen to travel abroad to engage in sexual activity with any child under the age of 18 (18 U.S.C. 2423(b)). Individuals who partake in this illegal activity are subject to prosecution in the United States even if they committed the crime on foreign soil.

Child Sexual Molestation (not in the family)

Child sexual exploitation (not in the family), also known as extra-familial child sexual abuse, includes all sexual exploitation of a child by someone other than a family member.

Unsolicited Obscene Material Sent to a Child

It is an unfortunate reality of the Internet that children will encounter obscene material online. Many times this material is attached as an image(s) or hyperlink(s) sent to a child in an unsolicited E-mail or 'spam'.

To combat this problem NCMEC takes reports of unsolicited obscene material sent to a child. It is a violation of criminal law for any person to knowingly or attempt to send or transfer obscene material to another individual who has not attained the age of 16 years (18 U.S.C.A. 1470).

Please report any incidents where a child may have received visual depictions of persons engaging in sexually explicit conduct that is obscene.

If you are an adult who is concerned about adult obscenity not involving children on the Internet, please make a report to www.obscuritycrimes.org.

MISLEADING DOMAIN NAME

It is a federal offense to use a misleading domain name on the Internet with the intent to deceive a minor into viewing material that is harmful to minors, regardless of whether the material meets the legal definition of obscenity (18 U.S.C. 2252B). Please report the use of a misleading domain name that has directed a child to a web site containing harmful materials to children.

Adults who are concerned about obscenity that has not been accessed by a child on the Internet may file a report at www.obscuritycrimes.org.

HANDLING REPORTS

Any incidents reported to the CyberTipline online or by telephone go through this three-step process.

- CyberTipline operators review and prioritize each lead.
- NCMEC's Exploited Child Unit analyzes tips and conducts additional research.

- The information becomes accessible to the FBI, Bureau of Immigration and Customs Enforcement, and US Postal Inspection Service via a secure web connection. Information is also forwarded to pertinent state and local authorities and, when appropriate, to the Internet service provider.

PREVENTION AND EDUCATION

NCMEC also provides prevention and education resources to help keep children safer on the Internet and in the real world.

www.CyberTipline.com

Campaigns such as 'Help Delete Online Predators', 'Think Before You Post', and 'Don't Believe the Type' were produced, with the Ad Council, to help promote online safety and teach children and teenagers how to better protect themselves on the Internet.


www.NetSmartz.org

The NetSmartz Workshop is a program of NCMEC that uses age-appropriate, 3-D activities to teach children ages 5-17 how to stay safer on the Internet and in the real world. Parents, guardians, educators, and law enforcement have access to additional resources for learning and teaching children about online risks and how to avoid them. NetSmartz content is available to the public at no charge at www.NetSmartz.org and www.NetSmartzKids.org.

www.NetSmartz411.org

NetSmartz411 is parents' and guardians' premier, online resource for answering questions about Internet safety, computers and the Web. Adults can search the knowledge base for answers to all of their questions about the online world! If they can't find what they're looking for, they can use the 'Ask the Experts' tab to send a new question.

The NetSmartz411 experts are highly trained, skilled professionals with an exceptionally high level of Internet knowledge. These full-time



employees of NCMEC go through a rigorous six-month training period to better understand all areas of the Internet and emerging technologies used by people looking to exploit children. This includes social networking websites, newsgroups, chatrooms, e-mail, instant messaging, online games, and peer-to-peer technologies.

Their primary responsibility within the Exploited Child Unit at NCMEC involves analyzing tips received through the CyberTipline.[®] The experts analyze the information and research individuals who groom and attempt to sexually exploit children online as well as those that victimize children in the real world. They work closely with law enforcement and Internet industry leaders to stay one step ahead of these child predators.

Glossary and checklist



| | |
|---|--|
| Acceptable use policy/terms and conditions | <p>An acceptable use policy is a set of rules applied by many transit networks which restrict the ways in which the network may be used. Acceptable use policies are used by concerns and companies with a large user base and multiple computers, delimiting what is and is not permitted for use of the computers. Most providers of services on the Internet include an acceptable use policy as one of the key provisions of their terms and conditions.</p> <p>Terms and conditions of service make clear what is permitted or not when using a product or service.</p> |
| Algorithm | A set of rules applied to the search engine's database which determines the order in which websites are listed in search results. |
| Blog | Short for weblog. An online journal (or newsletter) that is frequently updated and intended for general public consumption. |
| CEOP | The Child Exploitation and Online Protection Centre – the primary law enforcement authority in the UK for child protection on the Internet. |
| Cookie | A piece of information sent to a user's computer by a website. The computer then returns that information to the website. This is how some websites 'remember' a user's previous visits. |
| Database | An electronic store of information usually categorised and ordered into a holding structure. |
| ECPAT | End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes – a network of organisations and individuals working together to eliminate the commercial sexual exploitation of children. |
| FAQs | Frequently asked questions. |
| Full profile | The web page(s) where a user can publish personal information about themselves for people to better understand who they are. A 'full' profile will contain all the options the service provider makes available to users in terms of data fields and plug-in applications (where available). A user can pick and choose which data fields to complete and which applications to display and use on their page(s). A full profile differs from a search result, which would display only very limited information such as name and photograph. |
| Grooming | Actions deliberately undertaken with the aim of befriending a child, in order to lower their sexual inhibitions or establish an intimate friendship in preparation for the eventual introduction of sexual activities with them. |

| | |
|--------------------------|---|
| Happy slapping | <p>A fad in which an unsuspecting victim is attacked while an accomplice records the assault (commonly with a camera phone). The name can refer to any type of violent assault, not just slapping – even rape and sexual assaults have been classified as ‘happy slapping’ by the media.</p> <p>Originally, the defining feature of happy slapping was an effort by the attacker to make the assault seem like play, though some happy slappers indulge in extreme violence.</p> <p>Often those found performing such activities will say they were just ‘happy slapping’, asserting that they were just kidding.</p> |
| Hosting | <p>Hosting refers to the housing of a website. A website must physically reside on a computer (a server) which is connected to the Internet to ensure that it is available online.</p> |
| Instant messaging | <p>A form of real-time communication between two or more people based on typed text. The text is conveyed via computers connected over a network such as the Internet.</p> |
| IP address | <p>Internet Protocol address – a unique address that certain electronic devices use in order to identify and communicate with each other on a computer network utilising the Internet Protocol standard – in simpler terms, a computer address.</p> |
| IWF | <p>The Internet Watch Foundation – the only recognised non-statutory organisation in the UK operating an Internet ‘hotline’ for the public and IT professionals to report their exposure to potentially illegal content online.</p> |
| Link/hyperlink | <p>Hyperlink (often referred to as simply a link) – a reference or navigation element in a document to another section of the same document, another document, or a specified section of another document, that automatically brings the referred information to the user when the navigation element is selected by the user.</p> |
| Malware | <p>Software designed to infiltrate or damage a computer system without the owner’s informed consent. It is a portmanteau of the words ‘malicious’ and ‘software’. The expression is a general term used by computer professionals to denote a variety of forms of hostile, intrusive or annoying software or program code.</p> |
| Moderation | <p>The monitoring and filtering of user-generated content by human or technical means.</p> |
| Moderator | <p>A moderator may remove unsuitable contributions from the website, forum or Internet Relay Chat (IRC) channel they represent in accordance with its moderation policy.</p> |
| MSISDN | <p>The Mobile Station Integrated Services Digital Network – the mobile equivalent of ISDN.</p> <p>MSISDN refers to a unique number that is used to refer to a subscription in a particular mobile device.</p> |

| | |
|----------------------------------|--|
| Navigation | The act of moving from one area to another within a website, or between websites, by clicking on links. |
| Network | A group of interconnected computers capable of exchanging information. The Internet is a network. Most offices operate computers within a network. |
| NSPCC | The National Society for the Prevention of Cruelty to Children – a UK charity working in child protection and the prevention of cruelty to children. |
| PDA | Personal digital assistant. A hand-held electronic device which may include the functionality of a computer, mobile phone, music player and camera. |
| PIN | Personal identification number. |
| Profile | A profile is an easy-to-create webpage which contains personal information a user gives about themselves in order for people to better understand who they are. It can include all kinds of information, including some ‘sensitive’ information such as sexual orientation, religion, etc., and it is therefore important that users understand what other users can see. |
| Server | A computer on a network which is dedicated to a particular purpose and which stores all information and performs the critical functions for that purpose. |
| Social networking | A social networking site is an online community where people from all over the world can meet and share common interests. There are several hundred social networking websites. Most of them are free to join and allow users to set up their own personalised profile or blog. Often, users will list their location, age, gender and interests. Many social networking sites also allow users to post pictures, make comments on other people’s profiles or blogs, and search for other users. |
| Trojan | In the context of computer software, a Trojan horse is a program that contains or installs a malicious program (sometimes called the payload or ‘trojan’). The term is derived from the classical myth of the Trojan Horse. Trojan horses may appear to be useful or interesting programs (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed. |
| UKCGO | UK Children Go Online – research conducted by the London School of Economics and Political Science under Professor Sonia Livingstone. |
| URL | Uniform Resource Locator – another name for a web address. This indicates where a file, image or document can be accessed via the Internet. |
| User interactive services | Programs and applications which allow users to contact and interact with one another. |
| Virus | A computer program which distributes copies of itself, even without permission or knowledge of the user. To distribute itself, a virus needs to be executed or interpreted. Viruses often hide themselves inside other programs to be executed. |
| Website | A location on the World Wide Web, usually containing multiple webpages and normally owned by an individual, group, organisation or business. |

| | |
|------------------|---|
| Web 2.0 | A phrase coined by O'Reilly Media in 2004 to refer to a perceived or proposed second generation of Web-based services – such as social networking sites, wikis, communication tools, and folksonomies – that emphasise online collaboration and sharing among users. |
| Wikipedia | Multilingual, Web-based, free content encyclopedia project. <i>Wikipedia</i> is written collaboratively by volunteers, and its articles can be edited by anyone with access to the website. The name is a fusion or portmanteau of the words 'wiki' (a type of collaborative website) and 'encyclopedia'. |

| Requirements/recommendations for good practice checklist | | | |
|---|---|-------------|-----------------|
| Section 1: General principles | | | |
| 1.1 | All recommendations apply to all platforms, fixed or mobile | | |
| 1.2 | Each recommendation is seen as part of a larger focus on user protection. None of them is to be viewed as a panacea | | |
| 1.3 | Clear and relevant language and terminology for each target audience | | |
| 1.4 | Review and consider earlier Home Office Task Force recommendations | | |
| Section 2: Safety information, awareness and education | | | |
| | Requirement/recommendation | Date | Comments |
| | Safety information: | | |
| 2.1 | Is prominent, easily accessible and clear | | |
| 2.2 | Links are provided to relevant online safety and security resources | | |
| 2.3 | Includes user responsibilities | | |
| 2.4 | Is: | | |
| a | Specific to service provided | | |
| b | Up-to-date | | |
| c | Effective and relevant | | |
| 2.5 | Is available: | | |
| | During registration | | |
| | Prominently from the homepage | | |
| | Welcome email/message | | |
| | Other | | |
| 2.6 | Enables users to maintain privacy and prevent unwanted contact by providing instructions on: | | |
| a | Setting 'Ignore' function | | |
| b | Removing person from 'Friends' list | | |
| c | Removing other users' comments from their site | | |
| 2.7 | Includes instructions on how to submit a report/complaint to the service provider | | |
| 2.8 | See Section 10 below | | |
| 2.9 | Includes instructions on how to cancel an account and remove an unwanted profile | | |
| Section 3: Editorial responsibility | | | |
| | Requirement/recommendation | Date | Comments |
| | Editorial policy will include service approach to: | | |
| 3.1 | Careful judgement for use of under-18 profiles on homepage and encouraging other users to visit | | |
| 3.2 | Positioning of under-18 profiles alongside an adult theme | | |
| 3.3 | Ensuring advertising is appropriate for younger users and follows relevant local guidelines | | |

| Section 4: Registration | | | |
|--------------------------------------|--|------|----------|
| | Requirement/recommendation | Date | Comments |
| | During the registration process users are: | | |
| 4.1 | Informed how personal data will be used and what information will appear publicly on their profile | | |
| 4.2 | Protected by the service provider complying with legal requirements associated with obtaining consent from minors | | |
| 4.3 | Given the capability to protect or change any personal data that the service provider automatically makes public | | |
| 4.4 | Informed of what behaviour is and is not acceptable on the service (separately to the terms and conditions) | | |
| 4.5 | Informed of the implications of contravening the terms and conditions, that their activity is traceable and that the service provider will take action, including cooperation with law enforcement agencies where necessary | | |
| 4.6 | Required to provide personal information that can be validated | | |
| 4.7 | Traced by the capture of an IP address or MSISDN (this data is updated at each log-on, including time and date stamp) | | |
| 4.8 | Restricted from re-registering with false age details by uniquely identifying them by means of placing a cookie on their computer (or other technical measure), where they have previously attempted to register under-age details | | |
| 4.9 | Defaulted to a private profile (or user's approved contact list) if registering as under 18 | | |
| | OR pre-moderated prior to the profile being posted | | |
| | and limited to nickname, personal interests and general location only when creating a profile | | |
| 4.10 | Given control of any integration of existing contact lists or address books into a new list | | |
| 4.11 | Advised to review their contact list regularly | | |
| Section 5: User profile and controls | | | |
| | Requirement/recommendation | Date | Comments |
| | User profile tools provide users with: | | |
| 5.1 | Display devices to identify quickly the privacy status of their personal data (e.g. lock/key symbol) | | |
| 5.2 | The available options as to how/whether their profile appears in search results | | |
| | The ability to have a public profile that is not searchable via search engines | | |
| 5.3 | An acceptable behaviour message when uploading images onto their profile | | |
| 5.4 | Advice to under-18s on disclosing personal data | | |

Section 5: User profile and controls (continued)

| | Requirement/recommendation | Date | Comments |
|-----|---|------|----------|
| 5.5 | Advice on uploading data that may: | | |
| a | Identify their home address | | |
| b | Include other location information | | |
| c | Invade the privacy of others | | |
| d | Include inappropriate user names and images | | |
| 5.6 | The available options for adjusting privacy settings (on all aspects of the service) | | |
| | Service providers have: | | |
| 5.7 | Privacy settings that apply online presence or status to all integrated communication applications within the service | | |
| 5.8 | Considered a policy on reviewing and removing images that are inappropriate for an under-18 profile | | |
| 5.9 | Links in place to report abuse or flag user profiles | | |

Section 6: Search

| | Requirement/recommendation | Date | Comments |
|-----|---|------|----------|
| 6.1 | Private profiles of under-18 users are not searchable via service or search engines | | |
| 6.2 | Public profiles of under-18 users are not searchable using sensitive personal data fields, e.g. age, sex, location and school | | |

Section 7: Content screening and moderation

| | Requirement/recommendation | Date | Comments |
|-----|--|------|----------|
| 7.1 | Clear information is provided to reduce the risk of harassment or abuse, including how to: | | |
| a | Remove or block individuals on friends/contact list | | |
| b | Prevent posting of anonymous comments and remove unwanted postings from personal pages | | |
| c | Receive comments from users on friends list only | | |
| 7.2 | Consider user capability to pre-moderate/approve comments prior to posting (on all aspects of the service) | | |
| 7.3 | Consider adopting HO good practice guidance for moderation of interactive services for children | | |

Section 8: Age verification

| | Requirement/recommendation | Date | Comments |
|-----|--|------|----------|
| 8.1 | Review options for age-verifying users including the following: | | |
| a | Restricting from re-registering with false age details by uniquely identifying them by means of placing a cookie on their computer where they have attempted to register under-age details | | |
| b | Using algorithms to identify under-13 users who have falsified age details on registration | | |
| c | Offering free downloadable parental controls for the service | | |

| Section 8: Age verification (continued) | | | |
|---|--|-------------|-----------------|
| | Requirement/recommendation | Date | Comments |
| 8.2 | The risk of under-18 users accessing adult-themed content is minimised by: | | |
| a | Requiring users to tag such content as 'adult' | | |
| | Tagging such content as 'adult' by the service provider | | |
| | Dynamic filtering of content | | |
| b | Restricting access to content tagged 'adult' to those users registered as under 18 years of age | | |
| c | Using established age-verification system to validate those users registering as 18 and over | | |
| Section 9: Responsible use managing bullying via communications and other forms of abuse | | | |
| | Requirement/recommendation | Date | Comments |
| 9.1 | See Section 4.4 | | |
| 9.2 | See Section 2.1 | | |
| 9.3 | See Sections 2.6 and 7.2 | | |
| 9.4 | See Section 4.5 | | |
| 9.5 | See Section 2.7, 2.8 and 10.2 | | |
| 9.6 | Visitors are provided with the information and the capability to use the report abuse process (i.e. without being logged on to the service) | | |
| 9.7 | Service providers should highlight their information requirements within their report abuse process to facilitate effective handling of a complaint: | | |
| a | Reason for complaint | | |
| b | Location of content | | |
| c | Type of content | | |
| d | Date | | |
| e | Screenshot | | |
| f | Advice to save communications that cannot be sent to service provider, e.g. mobile text | | |
| g | Other | | |
| Section 10: Reporting concerns, abuse and illegal behaviour | | | |
| | Requirement/recommendation | Date | Comments |
| 10.1 | Clear and straightforward 'report abuse' process | | |
| 10.2 | Advice available on all applications and interfaces within the service and links to the reporting abuse process | | |
| 10.3 | Continue to research, develop and test ways of detecting suspicious behaviour towards children online | | |

Section 10: Reporting concerns, abuse and illegal behaviour (continued)

| | Requirement/recommendation | Date | Comments |
|------|--|------|----------|
| 10.4 | Consider a general report abuse page with links to report or discuss activities on the service, including: | | |
| a | The service provider | | |
| b | Law enforcement agencies | | |
| c | Emergency services via phone, when there is an immediate threat | | |
| c | Child welfare organisations | | |
| d | Confidential helplines/support services | | |
| 10.5 | Consider acknowledging each abuse report, confirming it will be managed and indication of timescale, if appropriate | | |
| 10.6 | Explore automating 'report abuse' process to capture essential information on the reported abuse | | |
| 10.7 | Provide the information and facilities necessary for users to report abuse directly to the relevant law enforcement agency | | |
| 10.8 | Continue reviewing direct reporting solutions for all media platforms | | |

Section 11: Reporting arrangements between service provider and law enforcement agency and child protection agencies

| | Requirement/recommendation | Date | Comments |
|------|--|------|----------|
| 11.1 | Service providers should establish reporting mechanisms with LEA to include: | | |
| a | Guidelines or protocols on what should be preserved as evidence | | |
| b | Protocols for disclosure that are compliant with relevant data protection and privacy legislation | | |
| c | Feedback mechanisms between industry and law enforcement | | |
| 11.2 | Continue to research, develop and test ways of detecting potentially illegal and/or suspicious behaviour towards children online | | |

