

Appendices

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES



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/UKCGOonlineliteracy.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

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES



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.
<i>Wikipedia</i>	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		

