Good practice guidance for the providers of chat services, instant messaging (IM) and internet connectivity content and hosting

Updated 2010

UK COUNCIL FOR CHILD INTERNET SAFETY

Contents

Overview

Part one: Chat

Part two: Instant messaging

Part three: Internet connectivity content and hosting

Overview

1. Introduction

The internet is transforming the way we live.

For children, in particular, it offers huge opportunities to communicate and to learn. It is fun; it is a great educational tool and it is enabling. Young people have embraced new technologies enthusiastically, especially the interactive services including games, chat, messaging, social networking sites and user generated content sites and made them their own. However, as highlighted in the Byron Review at www.education.gov.uk/ukccis, many parents and carers still lack confidence in the online space, and their use of these technologies differs from their children and young people. They often feel less technology literate than their children and unable to monitor their activities or to offer advice and support and are unsure how to teach their children about risk management skills. These parental anxieties are often compounded through the media's portrayal of technology-related stories which have linked anti-social criminal behaviours with technology use amongst children and young people.

However, alongside the huge legitimate benefits the internet offers there are potential risks for children, to reveal too many personal details about themselves, accidental exposure of children to inappropriate material, for bullying or harassment and, most seriously, for paedophiles to make approaches, for example, in chat rooms or via instant messaging, with the intention of "grooming" children for sexual abuse.

2. Purpose of this document

This document is part of a group of documents originally produced by the Home Office Task Force on Child Protection on the Internet, setting out a series of models of good practice for the provision of different kinds of internet services by a range of companies and organisations active in the online world.

These documents were intended primarily as a guide to commercial or other organisations, or individuals, who are already providing online services or are considering doing so in the future, but also as public documents of interest to internet users. These include:

- Good practice models and guidance for the internet industry on chat services, instant messaging and web-based services 2003, updated 2010
- Good practice guidance for the moderation of interactive services for children 2005, updated 2010
- Good practice guidance for search service providers and advice to the public on how to search safely 2005, updated 2010
- Good practice guidance for the providers of social networking and other user interactive services 2008, updated 2010.

3. History and background

The Home Office Task Force on Child Protection on the Internet (HOTF) was established in March 2001 in response to concerns about the possible risks to children after a number of serious cases where children had been "groomed" via the internet. In the face of such concerns, the Task Force was a unique collaboration bringing together, in a positive partnership, representatives from the internet industry, children's charities, the main opposition parties, government departments, the police and others who shared the aim of making the United Kingdom the best and safest place in the world for children to use the internet. The work of the HOTF was subsumed in the 2008 creation of the UK Council for Child Internet Safety (UKCCIS).

4. The UK Council for Child Internet Safety (UKCCIS)

UKCCIS brings together over 170 organisations and individuals to help children and young people stay safe on the internet. It was launched by the then Prime Minister Gordon Brown on 29 September 2008 and is made up of companies, government departments and agencies (including the devolved governments in Scotland, Wales and Northern Ireland), law enforcement, charities, parenting groups, academic experts and others. The Council was a recommendation in Professor Tanya Byron's report 'Safer Children in a Digital World,' March 2008.

UKCCIS has discussed and agreed the importance and value of the HOTF guidance documents, and has worked to update them in line with recent developments. The Good practice guidance outlined in these revised documents remains broadly the same, but it has been expanded to include developments like the Sexual Offences Act (2003) which introduced grooming legislation and the creation of the Child Exploitation and Online Protection Centre (CEOP) in 2006, as well as technological realities that were not present when the original guidance documents were written.

5. Child protection measures

Discussions in the Home Office Task Force groups highlighted the need for a range of measures to achieve agreed outcomes. It was agreed that practical steps by industry should be supported by increased awareness and supervision by parents and carers, ideally within a context of trust and agreed policies on acceptable internet use within the family. Less well-informed or engaged parenting would expose some children to higher degrees of risk, and it was agreed that various channels should be used to ensure that safety advice reaches as many children as possible. Overall, it was agreed that there was a clear need for standards to be raised to assist consumer awareness and choice and ultimately to help protect children.

6. Models of good practice

The criminal law applies equally to the internet as elsewhere: what is illegal off-line is illegal online. Within that framework, the Government has supported and encouraged effective self-regulation and models of good practice fit well within this approach. The models have been drawn up reflecting the general guidance above and examples of specific measures relating to the services that they cover. It is recognised that the "internet industry" is very diverse and ranges from large global providers to small locally run services. Many chat services are run by communities of internet users around particular issues or interests for example, so the models are not a "one size fits all" answer. The intention is that service providers – of whatever size – take from the models/guidance what they can. Many of the largest providers will already have in place much of what is suggested. The models are not intended to be prescriptive but are offered to the industry with a strong recommendation for their use.

The purpose of the best practice models is to:

- provide a framework of good practice for service providers to develop a better and safer service for users;
- help the industry to empower children and other users to make well-informed decisions e.g. about disclosure of personal details whenever they enter services or move between them;
- ensure clarity of information, warnings and advice, and
- strengthen public confidence in the services offered.

They are intended to be used alongside any legal obligations and other relevant codes, such as the code of practice for example relating to premium rate charged internet content and services operated by the premium rate regulator PhonePay Plus, the UK code of practice for the self-regulation of new forms of content on mobiles and the European Safer Social Networking Principles.

Part one: chat

1. Introduction to chat

Chatting online is popular with children and young users. However, engaging in online chat can leave young users open to a range of risks. The most 'headline grabbing risk' is the possibility of children being approached online by others with the aim of developing a sexual relationship with them in the 'real world' (contact). Online chat services also open children to other risks including exposure to inappropriate and hurtful conversations (content), being sent indecent or obscene images and being asked to send indecent images of themselves and/or their friends or being encouraged to self harm (conduct).

2. What is chat?

Chat typically starts in a public 'room' but can go private if the user chooses; the chat environment (in terms of who is chatting and what they can/can't do) is controlled by a provider and/or their moderator(s).

Chat is typically a real-time public discussion forum operated by a service provider and open to any user (registration and/or a profile may be required). Typically in chatrooms there are many users chatting together in real-time and although they may chat regularly online, they generally do not know each other offline. Users may have the option of moving to a private chat room to talk with one or more members of the public form. Where private chat is a one to one discussion, it may resemble instant messaging (IM) to the user.

As chat software has developed, individuals are not only able to send text messages to chat rooms but, are also able to communicate in real-time through voice chat, often using headsets, and be seen by other chat room members, through web cams.

Some chat services offer the user the ability to create a profile. A profile is a page that contains information about the user, and can provide a range of fields for such information as real name, location, age, and e-mail address, mobile phone number, personal website addresses, home address, interests and pictures/images. Other users can access this information and use it to contact and connect with people with similar interests

Chat services are also available on mobile phones and the mobile operators have signed up to a code of practice[1] to help parents control the type of content accessible to children. All commercial chat rooms must be placed behind access controls, where users verify they are over eighteen, unless they are moderated chat rooms. Additionally filters are made available for the wider internet on mobile phones.

Video games are also commonly played online and this online access provides shared playing places and allows users to chat together in real time. Multiplayer modes also allow users to chat and have a variety of interface game functions including chat and voice communications. Furthermore, there is a great deal of convergence with social networking services and service

[1] UK code of practice for the self-regulation of new forms of content on mobiles *Version 2 published 10th June 2009* http://www.mobilebroadbandgroup.com/social.htm

providers should refer to the good practice advice for the providers of social networking and other interactive services.[2]

There is a vast array of chat services, provided by companies running large global platforms, or individuals. Some are dedicated to particular interests, hobbies, news events, gossiping or simply to making new friends. Chat rooms run across a number of online and computer networks, such as:

- internet Relay Chat (IRC) is described as the 'Net's equivalent of CB radio.' IRC is not owned or run by any single organisation,
- web based chat on dedicated chat websites,
- chat can be offered by online publishers, including individuals e.g. bloggers, so that users can interact with each other or the editors,
- chat can be part of interactive online gaming environments and chat services are also accessible via internet-enabled devices including mobile phones and also on gaming devices,
- social networking sites, both as functions of those sites and as downloadable third party applications, and
- in online virtual worlds such as Second Life.

Chat is also used in the commercial world by companies as a means of communicating with their customers in real time to answer quick questions (e.g. in the context of a support service) or to offer advice (e.g. ask an online seller about a product). Likewise chat can be offered by a charity as a support service (e.g. CyberMentors provided by the charity BeatBullying and Childline provided by the charity the National Society for the Prevention of Cruelty to Children).

Chat comes in a variety of different forms. Often, when joining a chat service or room an individual must select an onscreen name, nickname or avatar, and all members of a chat room are usually listed down one side of the screen. As well as chatting in a specific room, individuals can request and initiate private conversations with other members of a chat room, which can appear similar to instant messaging. There are often facilities for individuals to break out into a private chat room and invite particular individuals to that chat room.

A number of chat services and programmes provide a range of tools for users, such as 'ignore' buttons if they are feeling harassed by a particular individual, or word filters which identify certain profanities and prevent them being displayed on a screen. Responsible chat providers offer reporting facilities so complaints can be made to the service provider about another chat user's behaviour if it is offensive or harassing. It is good practice to provide community guidelines setting out acceptable conduct, as well as links to resources offering advice and help about internet safety. The guidance below seeks to give general advice to cover the wide range of services on offer, and will therefore not be equally applicable to all providers.

[2] Good practice guidance for the providers of social networking and other user interactive services 2008 www.education.gov.uk/ukccis

3. Benefits of chat

Chatting online is a hugely popular activity for teenagers, and there are undoubted benefits in being able to communicate directly with people from around the world. Instant and real-time access to people of all ages and backgrounds enables the discussion of common interests, broadening horizons and increasing tolerance between both individuals and communities. All users, children and adults alike, can enjoy the opportunity to interact, regardless of ability, disability or discrimination which may affect them in the 'real' world.

4. Child safety concerns

Content

Children and young people can be put at risk through viewing and sharing inappropriate content via chat services, particularly through webcam chat services and the exchange of inappropriate files or links. Children may also be exposed to unsuitable language and may put themselves at risk by sharing too much personal information such as real name, address and phone number.

Specific concerns are that:

- chat services can be misused by individuals placing fake identities containing links to other sites, potentially exposing the user to porn and viruses,
- other users may make inappropriate material available by file transfer or live webcam images, and
- chat services can also be used to distribute spam messages.

Contact

Areas of the internet frequented by young people are often targeted by adults or adolescents seeking sexual contact with children.

- The real-time nature of chat services offers particular opportunities for direct and immediate contact, with the added facility to persuade a child to move to a private conversation.
- Chat can offer a predator or bully seemingly anonymous direct contact at a safe distance allowing contact to be made while the child is using the internet in the secure surroundings of their own home, even their own bedroom. This can give the opportunity for "grooming", the development of a trusting relationship by a paedophile with the intention of committing contact abuse at some point, and the potential for bullying to take place at any time, intruding into spaces previously regarded as safe user profiles and directories can allow a would-be bully or abuser access to personal information they may use to the detriment of the user as well as an opportunity to make initial contact; files or links accessed from messages in chat rooms may carry viruses, or other harmful content.

Conduct

Risks to children can arise from their conduct – where the child is the actor and thereby the agent of risk. This can include their engagement with commercial risk such as illegal downloading, hacking, gambling, or through their initiating or engagement with bullying/ harassing behaviour and through the creating or uploading of inappropriate content including personal information.

5. Chat good practice model

Chat services can be provided by a range of different agents who may wish to adopt some or all of the recommendations below; what is relevant will depend on the scale and nature of the service offered.

Product

Clear, prominent information should be displayed about the kind of service offered and the audience at which it is aimed e.g. is the chat room moderated or unmoderated? If moderated, what form of moderation is used? Is it aimed at a specific age group or type of person?

Safety advice

Clear, prominent and accessible safety messages should be present in appropriate places within the service, e.g. on front pages and in chat rooms themselves.

Safety messages should include information designed for both parents/carers or other adults, and children. Consideration ought to be given to providing the messages for children in language which will be accessible to all users the service is aimed at or likely to attract.

Information should be provided on service provider's own online safety guides and, where appropriate, on third party sites such as, www.chatdanger.com, www.childline.org.uk; www.childnet.com, www.direct.gov.uk/clickcleverclicksafe; www.kidsmart.org.uk, www.teachtoday.eu and www.thinkuknow.co.uk.

The user should be able to limit what personal information is made public and to control who sees what, for example, by the use of privacy settings. The need to utilise such tools should particularly be communicated to children, and they should be encouraged not to post their phone/mobile numbers, addresses, or e-mail addresses.[3]

Registration

Personal information gathered at registration should not be more extensive than is necessary. The purpose of information gathered, and uses to which it may be put, should be clearly and prominently explained.

[3] See section 4.9 Good practice guidance for the providers of social networking and other user interactive services 2008 www.education.gov.uk/ukccis

Tools

Service providers should deploy relevant safety tools and give due prominence to them within the service. These could include:

- ignore buttons;
- means of saving the conversation;
- report abuse mechanisms;
- advice on handling abusive chatters;
- filtering mechanism that might, for example, pick up bad language, or obscure certain characters such as numbers and @ symbol to prevent users giving out their phone number or email addresses;
- providing a means at the user end to block private chat/ instant messaging;
- privacy settings enabling the user to control who can access and see the information they have included in their profile. For example, settings might include private, friends only, friends of friends and public.

Service providers should deploy and give due prominence to a system of receiving and responding appropriately to reports of incidents. The reporting mechanism should be clear and accessible to the chat user, and the user should be informed of what to expect from the reporting process and a time frame for this, and their options for further action/appeal if not satisfied with the resolution.

Moderation

- In moderated chat rooms specifically aimed at or likely to attract children, service providers should consider deploying and giving prominence to a system for the user to alert the moderator.[4]
- All chat moderators should be properly recruited, screened, trained and supervised.[5]
- It should be clear to both the user of a service and also to the moderators themselves, what moderators are expected to do, and there should be a means of reporting failure to meet the user's expectations.
- Any chat provider needs to consider whether to allow users to post external links/URLs and how these should be moderated.

[4] See recommendation 10. Good practice guidance for the providers of social networking and other user interactive services 2008 www.education.gov.uk/ukccis

[5] In England and Wales it is an offence for a person who is on the children's barred list maintained by the Independent Safeguarding Authority to moderate a public electronic interactive communication service which is likely to be used wholly or mainly by children or engage in other 'regulated activity' in relation to children; for further information, see http://www.isa-gov.org.uk/. It is also an offence for an employer to engage a person for such work who they know or have reason to believe is barred. Enhanced criminal records certificates, including information on whether the person is barred, can be obtained for the purposes of employment which is concerned with the monitoring, for the purposes of child protection, of communications by means of the internet; for further information, see http://www.crb.homeoffice.gov.uk/ . The situation may differ in Scotland and Northern Ireland.

Part two: Instant messaging

1. Introduction to instant messaging

Instant messaging (IM) has become a positive mass communication tool as more and more people are coming online in the UK. As with any new technology, children have been quick to adapt and recognise the positive value of IM to enhance their lives, and 62% of 12 – 15s claim to use IM as part of their normal online activity.[6]

2. What is instant messaging?

IM typically starts privately and one-to-one but can be extended to *invited* users; the environment (in terms of who is chatting and what they can/can't do) is controlled by the user at all times.

IM is typically a one-to-one communication between two users in real-time but some IM services may allow users to invite other users to join their conversation and this may resemble chat to the users involved. However, the key difference from chat is that IM is a user-controlled environment and the user who initiates a conversation and/or opens up the call controls who can participate.

At its simplest, the technology provides an easy way of sending short written messages to one or a few friends online in real-time but IM can offer a range of communication tools, including: text-based chat, voice chat via voice over internet protocol (VoIP), webcams, and file and picture exchange. IM is a complex technology and can be accessed over a number of different platforms including: software clients, web-based systems, peer-to-peer, mobile phones and hand-held devices such as personal digital assistants.

There are many different IM products on the market, which are often freely downloadable from internet service providers' websites, or pre-installed on computers, games and mobile devices or accessible via services like social networks. Many social networking services have an IM type function, often called 'chat,' built in which enables the user to chat with their friends on the service. Although it is often confusingly called chat, it is more like IM as users chat one-to-one with individuals from their friends list.

IM can be a very private form of communication between known friends where the user builds up a list of contacts and is alerted when they are online. However IM users can also access public address lists to find and make new contacts online.

3. Registration

When obtaining IM products, service providers require users to register and provide a certain amount of personal information, for example, email address, personal

[6] Ofcom Media Literacy Audit: Report on UK children's media literacy 2008

websites, age, gender and location etc. This information may be transferred automatically to a 'member directory' or 'public profile,' which can be visible to other users and is sometimes shared with other services.

When registering for some IM services, it allows you to import contacts from other sources e.g. email address books and social networking friend lists.[7]

4. Public profile

A profile is a page that contains information about the user, and can provide a range of fields for such information as real name, location, age, e-mail address, mobile phone number, personal website addresses, home address, interests and images/pictures. Other users can access this information and use it to contact people with similar interests.

Although IM can be used as a private tool, information made public through IM can be used by anyone who sees it. People may be able to send messages to a user having found their profile in a profile search. However, the user may still have the option of either receiving such messages from unknown users or blocking them. Users can change or add to the personal information in their profile.

These profiles can operate in a similar way to social networking profiles, and privacy controls can allow individuals to keep their information private, share it with friends or make it public. Permissions can be set on each piece of profile information, making control very flexible.

5. Child safety concerns

Content

Children and young people can be put at risk through viewing and sharing inappropriate content via IM, particularly through webcams and the exchange of inappropriate links.

IM can also be used to exchange files or images on a peer-to-peer basis. This could include inappropriate and illegal content, which can be sent directly through file exchange or via unsolicited email (SPAM). Viruses and malware can be sent and have been used to corrupt and/or take control of users' computers, gaining access to all their files and potentially their webcams.

- Information should be available about how to keep safe in an online public environment for children, young people and parents, and in a style that is accessible to them. The messages should emphasise the importance of behaving responsibly online and what this means, including risks of communicating with strangers and/ or exchanging personal information such as name, address, school information and posting pictures.

[7] See 4.10 Good practice guidance for the providers of social networking and other user interactive services 2008 www.education.gov.uk/ukccis

Contact

Some concerns about IM stem, like telephone calls, from the private and unmoderated nature of the communication. Children have been quick to use IM and it has become part of their everyday lives to keep in contact with their friends at school or with friends they have made online. Children and young people have utilised the technology in positive and great ways but they too have realised its potential to harass and bully other young people, especially given the availability of mobile phones. Current research in this area reveals that cyberbullying is a feature of many young people's lives with the Staying Safe Survey 2009 (former Department for Children, Schools and Families) suggesting that 22% of young people reported being the target of cyberbullying.

Sexual predators have also recognised the power of IM to:

- operate in an environment of relative anonymity,
- move conversations from the public arena of chat rooms to a one-to-one private communication via IM,
- maintain contact with a child on their contact list, as they can always know when a child is online, and
- groom children with a view to isolating and manipulating them, developing emotional attachment and creating dependency in them, and meeting them in the real world.

Conduct

The way children behave when using IM can put them at risk. IM allows users to share files which could include images of themselves in response to requests/pressure from other users.

IM can offer easy access to and from other products, such as chat rooms, and can also be embedded in other products. Users can be just one click from the more private world of IM to the very public world of chat and vice versa. It is possible that some children may not appreciate the change in their environment. In some chat systems, the child's username for IM will be carried over to become the child's username in chatrooms, which then may make the user contactable via IM by someone who has seen them in a chat room. Parents themselves may not realise the integrated nature of IM and need to know about the potential risks of chat rooms, and that access to chat rooms can be easy.

6. Instant messaging good practice model

Product

- Clear information and description should be provided about what type of IM product is being offered to potential users e.g. about what it does and how it operates.

Environment

- The type of environment should be clearly described. For example, it should be clear whether it is an open community environment, for meeting people with similar interests, or a personal one-to-one environment to communicate with friends and buddies.

There should be ease of access to information about adjusting settings or managing preferences and privacy settings e.g. in order to only receive messages from friends or to block a particular user.

Advice

- Information should be available about how to keep safe in an online public environment for children, young people and parents, and in a style that is accessible to them. The messages should emphasise the importance of behaving responsibly online and what this means, including risks of communicating with strangers and/ or exchanging personal information such as name, address, school information and posting pictures.

- Clear and prominent messages about keeping safe online should be available for example on the home page for downloading IM and the IM client itself.

- Links should be provided to the service provider's own online safety guides and where appropriate to third party websites e.g. www.chatdanger.com, www.childline.org.uk www.childnet.com, http://clickcleverclicksafe.direct.gov.uk/index.html, www.kidsmart.org.uk, www.teachtoday.eu and www.thinkuknow.co.uk.

- If there is a public profile, clear and prominent safety messages should be visible highlighting the information which will be in the public domain in clear and prominent places.

- Safety messages should be visible when users receive a message from someone not on their friends/contact list or when they consider adding someone to their friends/contact list.

Tools

- Ignore or block features should be offered and clearly described on IM services so that users know how to deal with unwanted messages.

- Users should be offered the option not to receive incoming messages from people not on their friends contact list.

Reporting

- Features for reporting abuse, including how to address a breach of terms of service or community guidelines on acceptable behaviour, should be visible and easy to access on IM clients.

- Users should be made aware what types of abuse can be reported and what steps they can also take to help themselves.

- It should be easy for users to provide evidence of incidents of abuse e.g. accessing message history or screen grabs and so on.

- It should be easy for the user to provide information about an incident of abuse and its urgency when the report abuse mechanism is used.

- Service providers should deploy and give due prominence to a system of receiving and responding appropriately to reports of incidents. The reporting mechanism should be clear and accessible to the IM user, and the user should be informed of the response he/she can expect and a time-frame for this and their options for further action/further appeal if not satisfied with the resolution.

Reporting serious incidents

Information should be available to users about how to report urgent and serious incidents, including information about how to contact appropriate child protection and law enforcement agencies. See examples below:

- The Child Exploitation Online Protection Centre (CEOP) provides a public reporting tool online to deal with reported allegations and suspicions of any online or offline behaviour that suggests anyone under the age of 18 is being sexually abused or exploited by an adult or is at potential risk of such. See www.ceop.gov.uk.

- The Internet Watch Foundation (IWF) is the UK 'Hotline' for the public to report incidences of criminal content online. Its remit covers child sexual abuse images hosted anywhere in the world, criminally obscene adult content hosted in the UK, incitement to racial hatred content hosted in the UK and non-photographic child sexual abuse images hosted in the UK. For more information or to report content, see www.iwf.org.uk. If or where there could be an immediate risk to life, users should be advised to dial 999.

Privacy

- Users should have clear guidance about how much personal information will be publicly available.

- At registration, if personal information is required, the user should be informed how this information will be used within the service and by third parties if relevant.

- Registration details should not automatically transfer to public profiles or open member directories.

- There should be clear links to the company's privacy policy.

- Users should be made aware what information is publicly accessible from their profiles and be given advice about the potential risks of sharing personal identifying information and thus potential contact with unknown people. User consent should be required where the provider offers to 'scrape' contacts from other sources including the user's email address books and social networking friend lists. These 'importing' functions

should remain under the user's control.[8]

[8] For more details see 4.11 in the Social Networking Guidance www.education.gov.uk/ukccis

Part three: internet connectivity content and hosting

1. Introduction

These guidelines address a number of issues that touch on or concern children's safe use of the World Wide Web, or "the web" as it is more commonly known.

Addressing child safety on the web is complex. The web is used by all kinds of individuals, companies and organisations, to present all types of material about them, their organisation or their interests.

This document is intended for those who provide services or publish content that appears on the web, and also those who facilitate that publication or provision e.g. internet connectivity providers and hosting companies. However, it is also hoped that the guidelines and the recommendations it contains will be of interest to consumers of web content and services, particularly those who supervise children's access to the internet e.g. parents and teachers.

There are websites that are not specifically aimed at children but which, common sense and experience suggest, are very likely to attract children to them, e.g. sites linked to sports events, games or sites connected with rock bands or fashion. Companies or organisations responsible for such sites ought to consider to what extent relevant and appropriate elements of this good practice guidance might usefully be followed or adopted.

2. Definitions

Content providers: anyone who publishes via the Web, whether they be a commercial company, other kind of organisation or an individual. This will include portals and search engines, company websites, advertisers and other organisations or institutions, and individual web-users who have web space. Some organisations fall under this heading in respect of only some of their activities, such as internet connectivity or hosting providers which publish their own material.

Connectivity providers: companies that provide access to the internet including Internet Service Providers (ISPs) and mobile network operators.

Hosting providers: companies who provide web space. This may include companies who also provide internet access or, for example, educational institutions, which own and manage their own servers for hosting content.

Web-users: Children, parents, carers and the public at large who access the Web.

The Good Practice Guidance is primarily aimed at the internet industry in the UK. The aim is to develop and share guidance that will help protect children without reducing the opportunities it offers, and which encourages safe use of the internet. We hope that all users of web services, whether these descriptions apply to them or not, will consider the issues and ideas set out here. We would encourage providers to consider whether their customer base includes children or families.

3. Child safety concerns

Content

There is no dispute that illegal content (such as child abuse images) is a serious concern for all of us. However, children also need to be protected from a wider range of legal content that may be acceptable for an adult to see but which is clearly unsuitable for younger people. This may include, for example, material encouraging self harm or explicit sexual and violent material.

Contact

Risks to children can arise from the misuse of web services by ill-intentioned individuals seeking to make contact with them. Such individuals will seek out interactive areas of the web where they are likely to make contact with children. Children using such areas need to be aware of the risks and encouraged not to give out personal information that may identify them and place them at risk such as in chat rooms, instant messaging services, member directories, profiles or personal web pages.

Commerce and privacy

Children can be vulnerable to advertising that is not clearly marked as such, for example advertising which appears to be editorial content. Advertising can also exploit children through their lack of experience and maturity.

Risks to children may arise from the misuse of their personal data. Children may willingly provide their and others' personal information without being aware of the implications, for example, in order to enter competitions, and this information can be open to misuse. At the very minimum, the standards set by the Information Commissioner must be upheld.[9]

4. Internet connectivity content and hosting good practice models

Content providers

1. Web users should be helped to understand what kind of content they are going to access, for example clear signposting of what the content is and who the content is for, so as to avoid offending users or taking them by surprise.

2. Websites specifically aimed at or likely to attract children should ensure that content on their site is suitable for their audience. Sites should ensure that they offer navigation which does not lead younger users from content which is suitable for them e.g. on a general portal's home page, directly to content which is clearly unsuitable.

[9] Information Commissioner, www.informationcommissioner.gov.uk

3. Users of children's sites should be clearly informed when they are about to move to third party content.

4. Particular attention should be paid to hyper-linking to third party sites from sites aimed at or likely to attract children. The content of the third party sites should be checked for suitability initially. There should be arrangements in place to deal with unsuitable links, e.g. through contracts with the third party or complaints systems. Where appropriate a warning or notice should be provided to make it clear to the user that they are about to be transferred to an 'external' site.

5. Content providers should follow the rules of the Data Protection Act and any associated legislation, regulations and guidance when handling data collected from their website.[10]

6. In addition to complying with data protection legislation, websites that collect personal data should provide a privacy statement, which includes details about what information is collected when someone visits the site, and what will happen to that data. This will include information about cookies, web logs and specific data entered whilst using the site (e.g. for competitions).

- Children's privacy should be protected. The level of protection will depend on several factors, for example, the intended use of personal information gathered and the age of the target audience.

- Websites that collect information from children may have to put more rigorous safeguards in place to ensure that the processing of those children's information is fair.

- Website operators should recognise that children generally have a lower level of understanding than adults and notices explaining the way their data will be used should be appropriate to this level of understanding of the target group and should not attempt to exploit any lack of understanding.

Guidance from the Information Commissioner[11]

Information about children

Understanding, rather than age, is the key to ensuring the fair treatment of children when collecting and using personal data about them. However, it is good practice to obtain parental consent before collecting personal data from children aged under 12.

Relying purely on age involves many practical difficulties, in that the reliable online identity and age verification mechanisms needed to determine age are often not in place. Even if they were in place, it could be fairly easy for a determined child to circumvent them.

It is clear that certain services are aimed at particular age groups, for example children of primary school age or those in their late teens. It is good practice for the providers of such services to ensure that they only collect personal data in a way that their core audience is likely to understand. In short, this means only simpler propositions are acceptable for younger children, more complex ones for older children.

Parental consent

[10] Information Commissioner, www.informationcommissioner.gov.uk

[11] ICO's 'Personal Information Online code of practice' http://www.ico.gov.uk/ebook/ebook.htm

In general, a parent can legitimise the processing of personal data about his or her child by giving consent for this. It is good practice to seek parental consent where the collection or use of information about a child is likely to result in:

- *disclosure of a child's name and address to a third party, for example as part of the terms and conditions of a competition entry,*
- *publication of a child's image on a website that anyone can see,*
- *making a child's contact details publicly available, and*
- *the collection of personal data about third parties, for example where a child is asked to provide information about his or her family members or friend.s*

The key issue is to take into account the degree of risk that the collection or use of the personal data poses to the child or to others.

Obtaining reliable, verifiable parental consent can be extremely difficult or impossible. One problem is that it is the child accessing the service that will be asked to provide his or her parents' details. This could allow the child to provide false parental details, for example by setting up a bogus email contact address. The promise of a prize or other inducement could encourage resourceful children to do this.

If you cannot obtain verifiable parental consent, for example by talking on the telephone to a child's parent, and the information you intend to collect could put a child or others at risk, you should not collect the information.

Information about third parties

Sometimes children are asked to provide information about other people, for example their friends or family members. If they do provide this information, it is good practice to contact the individuals concerned as soon as possible to inform them that you have their details, to tell them what they will be used for and to delete them if they object or fail to respond to your communication.

7. The Committee of Advertising Practice (CAP) code has specific rules about children that apply online as well as offline. Examples of these can be seen below:

- Advertisements and promotions addressed to or featuring children should contain nothing that is likely to result in their physical, mental or moral harm.

- Advertisements and promotions addressed to, or featuring children should not exploit their credulity, loyalty, vulnerability or lack of experience.[12]

8. Content providers are encouraged to consider self-labelling (i.e. describing the content of their site) with PICS compatible systems. It is acknowledged such systems need further development but they can play an important part in dealing with content issues.[13]

9. Websites aimed at or likely to attract children should advocate safe surfing and provide links to suitable safety advice.

[12] See Advertising Code http://bcap.org.uk/The-Codes/CAP-Code.aspx
[13] PICS http://www.w3.org/PICS/. http://www.fosi.org/icra/

10. Websites should be careful about including photos, contact or other details, which together could serve to make children identifiable and contactable.

11. Providers of content aimed at or likely to attract children should also provide a contact address or reporting mechanism for complaints and act upon them as appropriate.

12. Content providers should consider whether it would be beneficial and relevant for them to work with the industry's self-regulatory body, the Internet Watch Foundation (IWF), in order to support and develop their work minimising the availability of criminal content online including provision of the 'notice and takedown' service for child sexual abuse content, criminally obscene adult content, incitement to racial hatred content and non-photographic child sexual abuse images hosted in the UK.

User-generated content

In addition to social networking services which have been covered separately and previously in the Good Practice Guidance for the providers of social networking and other user interactive services 2008 (updated 2010) document, a number of content providers allow web users to add material to their website, for example through message boards otherwise known as bulletin boards, or via web chat. Where such providers become aware of material that may be considered illegal they may be held liable for its continued presence.

1. Content providers who provide facilities for users to contribute material to the sites should consider the following:

- steps to ensure that illegal content, or content that is the subject of justified complaint by other users, can be identified and removed,

- that websites aimed at or likely to attract children should have a means of identifying and removing content that is unsuitable for their expected audience, including providing a means to the user for making a complaint or report,

- that message and bulletin boards or forums aimed at or likely to attract children may wish to pre moderate all user-generated content so that all material is seen and checked before it is published, and

- provision of a post-moderated service if the service is aimed at older children – where messages will be removed by a moderator once published, if the posts are clearly in breach of house rules on e.g. the publication of personal information.

2. Interactive web services can, if misused, provide the means for children to receive inappropriate and potentially harmful content and even contact by other users for ill-intentioned and inappropriate purposes. To empower the users of these services, so that they may keep safe, web sites which run bulletin boards or other places where third party content is present, should consider providing:[14]

- a facility to easily report abuse and misuse of the service, including help on how to log or record abuse so that a report can be acted on effectively,

[14] See good practice guidance on Chat and Instant Messenger for further details on good practice with interactive services www.education.gov.uk/ukccis

- house rules in interactive areas designed for children where the publication or exchange of personal information is not allowed and where users' contributions in breach of these rules will not be posted or will be removed once posted,

- advice on online safety, perhaps by linking to third party sites which provide this type of information, and

- information about profiles and advice about the risks of revealing personal information so that it can be seen by other users.

3. Web sites aimed at or likely to attract children offering search engine facilities should consider providing and promoting "child friendly" searching.

Providers of adult content

There are very real concerns about certain practices within some sections of the adult entertainment industry which impact children. These include, but are not limited to, the following:

- unsolicited e-mail advertising their content which is being sent to large numbers of email addresses, including those belonging to children,

- the launching of multiple windows, when a web page is loaded,

- the placing of explicit graphic sexual material on the front page of a web site, or

- advertising content so an inadvertent visitor will be exposed to this material.

There is a particular responsibility on providers of adult content to protect children by taking the following steps:

- Holding their content behind a page requiring clicking on an 'I am 18' button or equivalent in order to proceed to it. The 'public' front page should not contain explicit graphics or text, but rather should make clear that the site contains sexual material that is unsuitable for children and young people.

- Considering using age-verification systems to prevent children and young people accessing the site.

- Not promoting their websites through unsolicited email without the prior consent of the recipient. Some companies operate opt-in lists.

- Making it easy to leave the website/s without being constantly redirected.

- Refraining from launching multiple windows.

- Not using deceptive domain names of interest to children to get traffic, for example misspellings (e.g. dinsey.com) and similar names/ URLs.

Connectivity providers

1. Connectivity providers should provide information to their home users on their front page or through prominent links to help parents to:

- understand the risks of the technology their children may be using,
- take steps to communicate clearly with their children about possible dangers and safe ways of using the internet,
- take practical steps at home to help their children stay safe online, for example by placing the PC in a common area in the home and monitoring their use of the internet,
- enable and disable internet connectivity on mobile and gaming devices and understand what safety features are provided and how they can be utilised, and
- understand the availability, use and limitations of filtering and monitoring software, along with clear guidance on its use and the safeguards it does and does not provide.

2. Connectivity providers should ensure that their users have access to guidance on 'safe surfing.' They should consider providing guidance suitable for several different audiences, for example, parents who may not be internet literate and for the children themselves.

3. Connectivity providers should have effective mechanisms for dealing with complaints relating to their users' use of websites.

4. Terms of service should make clear the limits of acceptable online behaviour, and that unacceptable behaviour may lead to withdrawal of service and possibly referral of incidents to law enforcement agencies.

5. Connectivity providers should consider warning users that they have legal liability for content they place on the web. Posting material online on someone else's website, or in a web-based chatroom for example, is subject to the law just as publishing material in print is. Posting illegal material, threats, or harassment brings the risk of prosecution.

6. Connectivity providers that focus on the home market should consider providing the option of filtering software or filtered services to their users.

7. Connectivity providers should consider working with the industry's self-regulatory body, the Internet Watch Foundation (IWF),[15] in order to support and benefit from their work minimising the availability of criminal content online including their provision of a list of URLs depicting child sexual abuse which protects users from inadvertent exposure to such content. The deployment of this list is also a requirement of the Office of Government Commerce (OGC) for suppliers of internet services to national and local government.

8. Connectivity providers should inform users they can make a report to the IWF about content they believe may be criminal and which is within the IWF's remit. They may also wish to provide a hyperlink to the IWF site.

[15] www.iwf.org.uk

9. They should also inform users they can make a report about suspicious sexual behaviour towards a child, to CEOP and provide a link to the CEOP site.[16]

Hosting providers

1. Hosting providers offering services to home users should provide clear and timely guidance and advice to customers, especially children and young people, about creating web pages. Such advice should include making users aware that creating “home pages,” publishing personal details such as telephone numbers, address for email, home, school, and photographs could make them easy to identify, and trace, and could result in ID theft.

2. Terms of service should make clear the limits of acceptable online behaviour, and that unacceptable or abusive behaviour will lead to withdrawal of service and possibly referral of incidents to law enforcement agencies.

3. Hosting providers should make clear in their Terms of service or Acceptable use policy (AUP) that their customers have legal obligations of their own regarding certain types of content.

4. Hosting providers should have effective mechanisms for dealing with complaints about their customers’ websites.

5. Hosting providers should encourage content providers to consider self labelling (i.e. describing the content of their site) with PICS compatible systems. It is acknowledged such systems need further development but they can play an important part in dealing with content issues.

6. Hosting providers should ensure that they provide the IWF with a contact point to receive notifications about criminal content held on their systems and have a procedure in place to remove it in a timely manner.

[16] www.ceop.gov.uk