



Home Office

BUILDING A SAFE, JUST  
AND TOLERANT SOCIETY

## Home Office task force on child protection on the internet

Good practice models and  
guidance for the internet  
industry on:



CHAT SERVICES



INSTANT MESSAGING (IM)



WEB BASED SERVICES



**Home Office**

BUILDING A SAFE, JUST  
AND TOLERANT SOCIETY

# Home Office task force on child protection on the internet

Good practice models  
and guidance for the  
internet industry on:

**Chat Services**

**Instant Messaging (IM)**

**Web Based Services**

## Contents

• Foreword	3
• Introduction	4
• Good Practice Model for Providers of Chat Services	10
• Good Practice Model for Providers of Instant Messaging Services	16
• Good Practice Model for Providers of Web Based Services	21
• Members of Sub-Group F and Project Teams	31

If you have any comments or queries about the models please contact:

**David Ware**  
**Sentencing and Offences Unit**  
**Home Office**  
**50 Queen Anne's Gate**  
**SW1H 9AT**  
**Tel: 020 7273 2783**  
**Fax: 020 7273 4345**  
**e-mail: [david.ware@homeoffice.gsi.gov.uk](mailto:david.ware@homeoffice.gsi.gov.uk)**

### Foreword by Hilary Benn MP Chair, Taskforce on Child Protection on the Internet

I am delighted to be able to launch these models of good practice for the internet industry on behalf of the Task Force on Child Protection on the Internet.



The Task Force was established by the previous Home Secretary in March 2001 to consider what could be done to tackle serious child protection issues which were emerging with the increasing popularity of the Internet, in particular the potential risk of paedophiles contacting children through chat rooms and other on-line communications.

The Task Force partners – child welfare organisations, the internet industry, the Government, the police and others – have worked together to find solutions which will make the Internet a safer place for children without diminishing their enjoyment of the exciting opportunities which it offers. We have run a successful education and awareness campaign which is about to be repeated; the Government has announced its proposals for legislation to increase the armoury of the law against paedophiles. The models of good practice, which are launched today, offer guidance to the internet industry on how they can play their part in raising standards to improve child safety.

The models are intended to be of practical help to providers of internet services, and cover chat, instant messaging and web based services. They are voluntary and, as such, depend for their success on wide take-up within the industry. We are leading the world in producing these models of good practice and have an opportunity to influence developments in child safety beyond the UK. They represent a substantial achievement and I am grateful to everyone involved for the time and effort which they have given to answering this challenge. Because they are a new development, we will be reviewing them and will welcome feedback on them in due course.

I strongly recommend the models and urge all sectors of the internet industry to consider how they can be applied, whether in whole or in part, to their services.

A handwritten signature in black ink, appearing to read 'H. Benn'.

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 the new technologies enthusiastically, especially the interactive services like games, chat and messaging and made them their own. However, parents and carers often feel left behind, less technology – literate than their children and unable to monitor their activities. A recent research study showed that parental thinking about the Internet was much less developed than for television, but as a medium it raised more concerns and uncertainties<sup>1</sup>.

Alongside the huge legitimate benefits the internet offers, there is the potential for accidental exposure of children to pornographic or paedophilic 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.

### **Purpose of this document**

This document sets out a series of models of good practice for the provision of different kinds of internet services by a range of companies and organisations who are active in the online world. It is 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. As a public document, it will also be of interest to internet users.

It was prepared by the Home Office Task Force on Child Protection on the internet, a unique collaboration between the internet industry, Government and main opposition parties, law enforcement and children’s interests.

<sup>1</sup> “Striking a balance: the control of children’s media consumption”, edited by Pam Hanley, Head of Audience Research, ITC (commissioned by the BBC, BCC and the ITC)

## Home Office Task Force

The Home Office Task Force on Child Protection on the internet was established in March 2001 in response to concerns about the possible risks to children after a number of serious cases where children had been “groomed” via the internet. This is where a paedophile makes contact with a potential victim and uses a range of techniques to gain their trust and develop a relationship with the intention of sexually abusing them. Relationships may be established over a period of months or even years. Paedophiles may seek employment which brings them into close contact with children; they may also make use of a range of communication tools such as chat, emails and mobile phones.

In the face of such concerns, the Task Force brought together, in a positive partnership, representatives from the internet industry, children's charities, the main opposition parties, government departments, the police and others who share the aim of making the United Kingdom the best and safest place in the world for children to use the internet. A sense of shared responsibility underpins the work of the Task Force and an acknowledgement that each of the groups represented has a part to play.

The Task Force set up a number of sub-groups to focus on issues around: the criminal law, law enforcement, training, industry standards and co-regulation, child protection measures and education and awareness.

## Work of the Sub Groups

Most paedophile activity is covered by current legislation. However, the Criminal Law sub-group has developed proposals which will tackle predatory behaviour before a sex offence has taken place where there is evidence of an intention to abuse. This will apply offline as well as online. Separately, the framework of the law and penalties for sex offences is also under review. The Government set up the Sex Offences Review in 1999 and their recommendations were published for public consultation in ‘Setting the Boundaries’ in July, 2000<sup>2</sup>. The purpose of the

<sup>2</sup> “Setting the Boundaries – Reforming the law on sex offences” published by Home Office Communication Directorate July 2000.

Review is to modernise and strengthen the law, to provide coherent and clear sex offences which protect individuals, especially children and the more vulnerable, from abuse and exploitation. The Government has announced its intention to legislate in these areas in the next parliamentary session.

A national awareness campaign for parents/carers and children was launched in December/January 2001/2 and ran until Spring 2002. This stressed the benefits of the internet while raising the awareness of children and their parents/carers about its potential abuses and of the simple steps which children can take to protect themselves online. The Task Force is working to repeat the campaign early in 2003.

Work is being taken forward to ensure that the police have the expertise to tackle cybercriminals and that all practitioners in the area of child protection are internet aware. Training courses have been developed and are being run for specialist law enforcement officers by the National Specialist Law Enforcement Centre, who have also piloted an awareness module for all police probationers which will be part of the probationary training of all police officers. The Task Force is now looking at awareness training for child protection workers.

A sub group has also looked in detail at practical measures which can be taken to ensure that children can use the internet more safely. The outcome of that group's work is set out in this document. It is the result of considerable effort by the whole group and the project teams whose membership is listed on pages 31 and 32.

### Child Protection Measures

Discussions in the sub group have highlighted that there is no single answer to protecting children as they explore the potential of the internet. There is a need for a range of measures such as rating and filtering software, like that provided free of charge by the internet Content Rating Association (ICRA)<sup>3</sup>, and better signposting of potentially harmful material. But technical measures are not foolproof. They have to be supported by increased awareness and supervision by parents and carers, ideally within a context of trust and agreed policies on

<sup>3</sup> ICRA [www.icra.org](http://www.icra.org)

acceptable internet use within the family. Less well-informed or engaged parenting will mean that some children face higher degrees of risk. Thus, various channels should be used to ensure that safety advice reaches as many children as possible.

The sub group has looked at the services to which children are most attracted and which offer the greatest potential risks either of access to unsuitable material or of unwanted, possibly ill-intentioned, approaches by others: chat services, instant messaging and web based content. The group has also considered the difficulties posed by unsolicited emails (SPAM) and will be publishing separate guidance for consumers on this subject.

In looking, in particular, at chat and instant messaging services, the group recognised the immense potential benefits of the technology and its obvious popularity with children. It also recognised the wide variety of products available, some of which already incorporated user- friendly consumer protection measures. Overall, however, there was a clear need for standards to be raised to assist consumer awareness and choice and ultimately to help protect children.

## Clear Information

Common requirements have emerged in respect of chat, instant messaging and web services. Across all services, there is a need for clear, prominent, easily accessible information about the product offered and any relevant safety messages and safety tools. In particular, where users are invited to provide personal information e.g. at registration, it should be clear if the information will be in the public domain. The group identified obvious privacy and safety issues for all users in relation to the treatment of personal information at initial registration and in completing profiles, "buddy lists" etc.

***The Data Protection Act 1998*** is aimed at regulating the processing of information about individuals. The Information Commissioner is responsible for encouraging good practice in relation to the Act as well as having an enforcement role. More details about the Information Commissioner can be found at his website [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk).

<sup>3</sup> ICRA [www.icra.org](http://www.icra.org)

### Reporting Abuse

Mechanisms for reporting abuse should also be clear, easily accessible and easy to use. Reports should receive an appropriate response from a service provider's help centre. Information should also be available to users about how to report urgent and serious incidents of harassment or similar abuse.

### Models of Good Practice

In general, the criminal law applies equally to the internet as elsewhere: what is illegal off-line is illegal on-line. 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 specific measures relating to chat, messaging, email and web services. It is recognised that the "internet industry" is very diverse and ranges from large global providers to small locally run services. Many chat providers are community based, so the models are not a "one size fits all" answer. The intention is that service providers – of whatever size – take from them 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 models is to:

- provide a framework of good practice to deliver 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 mandatory requirements, such as the code of practice, relating to premium rate charged internet content and services, operated by the premium rate regulator, ICSTIS<sup>4</sup>.

## A World First

The Task Force has taken a significant step towards making the internet a safer place for children. Co-operation between the Government, the UK internet industry, the child welfare organisations, the police and others has produced models of good practice, which are the first of their kind in the world. But this is only a first step. The models will need to be acted on; they will also need to be updated as technology develops and reviewed in the light of feedback received on them.

<sup>4</sup> ICSTIS [www.icstis.org.uk](http://www.icstis.org.uk)

## Good Practice Model for Providers of Chat Services

### Introduction

A report published on internet chat services by the internet Crime Forum in March 2001<sup>5</sup> drew attention to “the possibility of children being approached on line by adults or adolescents with the aim of developing a sexual relationship with them in the ‘real world’ “. Such approaches can involve the assumption of a false identity, in particular the pretence of being a child, though this is not always the case. The report identified other risks to children, which may form part of this process: – children’s exposure to inappropriate conversation; unwittingly becoming the subject of sexual fantasy; being sent indecent or obscene images; being asked to send indecent images of themselves and/or their friends; being engaged in explicit sexual talk and/or being encouraged to perform sexual acts on themselves and/or their friends (so-called cybersex).

It recommended, amongst other things, increased levels of education and awareness among parents and other carers; responsible standards of care from providers of chat services for children, including the provision of clearly accessible safety tools and the provision of clear advice to all users about potential hazards and the nature and extent of protective measures offered by the service providers.

### What is Chat?

As access to the internet has grown in recent years, online chat has also become a huge social phenomenon both for adults and particularly amongst children and young people. Chat allows many people across the world to communicate directly by exchanging text, almost as if they were holding a conversation in a room with a group of people or on a one-to-one basis. As chat software develops, individuals are not only able to send text messages to chat rooms but, in some instances, also have the ability to communicate through their actual voices (voice chat) via headsets, or indeed, actually be seen by chat room members, through web cams.

There is a vast array of chat rooms, provided by major ISPs, companies running large websites, or individuals. Some are dedicated to particular interests, hobbies,

<sup>5</sup> ChatWise, StreetWise – Children and internet Chat Services, a paper prepared by the internet Crime Forum IRC Sub Group. [www.internetcrimeforum.org.uk](http://www.internetcrimeforum.org.uk)

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) which is described as the 'Net's equivalent of CB radio.' This is one of the most popular chat services on the internet. IRC is not owned or run by any single organisation.
- web based chat, which can be offered by ISPs such as BT or Freeserve, or Portals such as Yahoo! or MSN in the UK, with dedicated chat websites;
- chat can be offered by anyone with a website;
- chat can be part of interactive online role-play environments such as "Muds and Mushes", not dissimilar to the offline game of "Dungeons and Dragons", and
- chat rooms are also becoming accessible through mobile phones where dedicated chat channels have been created.

When joining a chat service or room an individual must select an onscreen name or nickname, 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 keys if they are feeling harassed by a particular individual, or word filters which eliminate certain profanities. Large chat providers offer reporting facilities so complaints can be made to the communication service provider about another chat user's behaviour if it is offensive or harassing. Community guidelines about conduct are often available, 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. A private chatroom run by an individual for a few well-known friends may require few measures: a large ISP with a wide range of popular chatrooms will need more.

## Good Practice Model for Providers of Chat Services

### Benefits of Chat

Chatting online is a hugely popular activity for teenagers. It gives them the chance to talk to existing friends and to meet new ones. The “Chat Wise, Street Wise” report noted that “There are undoubted benefits in being able to communicate directly with people from around the world. Instant and realtime access to people of all ages and backgrounds means that common interests can be discussed, horizons can be broadened, and tolerance increased between both individuals and communities. Children and adults alike can enjoy the opportunity to interact... Regardless of any disability or discrimination which may affect them in the ‘real’ world”.

### Child Safety Concerns

The negative side is the risk that areas of the internet where young people are likely to be found will be targeted by adults or adolescents seeking sexual contact with children, or, more widely, that inappropriate content or contacts will be made. Chat offers the predator anonymous contact at a safe distance allowing contact to be made even while the child is using the internet in the secure surroundings of their own home, even their own bedroom. This gives the opportunity for “grooming”, the development of a trusting relationship by a paedophile with the intention of committing later abuse.

Specific concerns are that:

- the realtime nature of chat offers particular opportunities for direct and immediate contact, with the added facility to persuade a child to go off into a private conversation;
- user profiles and directories can allow a would-be abuser access to very useful personal information, as well as an opportunity to make initial contact;
- other users may make inappropriate material available by file transfer or live webcam images;

- pornographic website operators can also misuse chat systems by placing fake profiles containing links to their sites, and sending messages with such links to other users, and
- files or links accessed from messages in chat rooms may carry viruses, dialler programmes linked to high cost telephone services, or other harmful content.

There have been a number of serious incidents where paedophiles have identified potential victims from among chat room participants and used a range of manipulative techniques to gain trust.

## Chat Good Practice Model

Anyone operating a chatroom may wish to adopt some or all of the recommendations below: what is relevant may depend for example on whether they offer IRC or web-based chat, or 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 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 both younger and older age groups.
- Links should be available to online safety guides in-house and/ or third party websites e.g. [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk), [www.chatdanger.com](http://www.chatdanger.com), [www.fkbko.net](http://www.fkbko.net), [www.childnet-int.org](http://www.childnet-int.org) and [www.nch.org.uk](http://www.nch.org.uk).

## Good Practice Model for Providers of Chat Services

- Clear and prominent safety messages should be visible when completing profiles, highlighting the information which will be in the public domain.

### 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.

### Public Profiles

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 and interests. It may give the opportunity to scan in and display a picture. Other users can access this information and use it to contact people with similar interests.

- The user should be able to limit what personal information about them is made public, and children should be made aware of the need for caution.
- Children in particular should be encouraged not to post their phone/mobile numbers, addresses, or e-mail addresses.

### Tools

- Service providers should deploy and give due prominence to some or all of the following safety tools:
  - ignore buttons; alert buttons; grab and print; reporting mechanisms;
  - advice on handling abusive chatters;
  - easy availability of filtering mechanism that might, for example, pick up bad language, or prevent children giving out their email addresses;
  - providing a means at the user end to block private chat/ instant messaging;

## Reporting

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 the response he/she can expect and a time frame for this.

## Moderated Chat

- In moderated chat rooms specifically aimed at children, service providers should consider deploying and giving due prominence to:
  - an alert system e.g. a panic/help button at the top of each chat room page.
- All chat moderators should be properly recruited, screened, trained and supervised: in the UK Criminal Records Bureau checks can now be made under the Rehabilitation of Offenders Act 1974 (Exceptions) Order on people who are in “employment which is concerned with the monitoring for the purposes of child protection of communications by means of the internet”<sup>6</sup>.
- It should be clear what moderators are expected to do, and there should be a means of reporting failure to meet the user’s expectations.

<sup>6</sup> Rehabilitation of Offenders Act 1974 (Exceptions) (Amendment) Order 2002, 5 (2) (c)

## Good Practice Model for Providers of Instant Messaging Services

### Introduction

#### Instant Messaging – a great technology

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<sup>7</sup>.

#### What is IM?

IM is a form of online technology allowing users to communicate in realtime with other users. At its simplest, the technology provides an easy way of sending short written messages to a few friends online at the same time but IM can offer a range of communication tools, including: text messaging, voice chat, webcams, and file and picture exchange. IM is a complex technology and can be accessed over a number of different platforms including: server-based systems, peer 2 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 companies' websites, or free sign-up CD ROMs offering internet access.

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. IM, however, can also be a public open environment where the user is encouraged to find and make new contacts online.

When obtaining IM products companies require users to register and provide a certain amount of personal information, for example, email address, personal 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 chat systems.

<sup>7</sup> A report by Pew internet and American Life Project, 'Teenage Life Online: The rise of the instant-message generation and the internet's impact on friendships and family relationships' (June 2001) found that in the US nearly three quarters of online teens between the ages of 12 and 17 (nearly 13 million) use IM. See <http://www.pewinternet.org/reports/toc.asp?Report=36>

## Public Profiles

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 and interests. It may give the opportunity to scan in and display a picture. Other users can access this information and use it to contact people with similar interests.

Though IM can be used as a private tool, information made public through IM can, with some products, be used by anyone who sees it. People may be able to send messages to a user having found their profile in a profile directory and seen that they were online. 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 the member directory or public profile.

## Child Safety Concerns

Some concerns about IM stem, like telephone calls, from the private and un-moderated 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 on-line.

Sexual predators, however, have recognised the power of IM to:

- operate in an environment of relative anonymity;
- make contact with children from member directories / profiles;
- 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

## Good Practice Model for Providers of Instant Messaging Services

- 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.

IM can also be used to exchange files or images on a peer 2 peer basis. This can include inappropriate and illegal content, which can be sent directly through file exchange or via SPAM. Trojan horses and viruses can be sent and have been used to corrupt and/or take control of users' computers, gaining access to all their files.

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 integration with mobile phones. Bullying can be continued online and beyond the playground when children are in the privacy of their own homes.

IM can offer easy access to chat rooms and vice versa. Users can be just one click from the more private world of IM to the very public world of chat, and 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.

### IM 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 preferences of the IM client to increase or decrease privacy e.g. in order to only receive messages from friends.

### **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 emphasize the risks of communicating with strangers and/ or exchanging personal information.
- Clear and prominent messages about keeping safe online should be available both on the home page for downloading IM and the IM client itself.
- Links should be available to online safety guides in-house and/ or third party websites e.g. [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk), [www.chatdanger.com](http://www.chatdanger.com), [www.fkbko.net](http://www.fkbko.net), [www.childnet-int.org](http://www.childnet-int.org) and [www.nch.org.uk](http://www.nch.org.uk).
- Clear and prominent safety messages should be visible when completing profiles, highlighting the information which will be in the public domain.
- Safety messages should be visible when users receive a message from someone not on their buddy list or when they consider adding someone to their buddy list.

### **Tools**

- Ignore or block features should be offered and clearly described on IM clients.
- Users should be offered the option not to receive incoming messages from people not on their friends / buddy list.
- Information should be available on how to deal with unwanted instant messages.

### **Reporting**

- Features for reporting abuse should be visible and easy to access on IM clients,
- Information should clearly describe what abuse should be reported and to whom, including inappropriate contacts, SPAM etc.

## Good Practice Model for Providers of Instant Messaging Services

- It should be easy for users to provide evidence of incidents of abuse e.g. archiving or screen grabs etc.
- It should be easy for the user to provide information about an incident of abuse and its urgency when the report button is pressed,
- When reporting abuse, users should receive feedback about what to expect in terms of a response from a company's help centre.
- If the response is automated it should state so clearly and indicate the time period within which a user will receive a response from the company.

### **Reporting serious Incidents**

- Information should be available to users about how to report urgent and serious incidents, including information about how to contact child protection and law enforcement agencies.

### **Privacy**

- Users should have clear guidance about what personal information they have provided is made publicly available.
- At registration with a company, if personal information is required, the user should be informed how this information will be used.
- Registration details should not automatically transfer to public profiles or open member directories.
- There should be clear links to the company's privacy policy.
- Profiles / member directories – users must know that this information is publicly accessible and be given advice about the potential risks of sharing personal identifying information and thus potential contact with unknown people.

## Good Practice Model for providers of Web Based Services

### Introduction

These guidelines address a number of issues that touch 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 web sites 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 whether or to what extent relevant and appropriate elements of this good practice guidance might usefully be followed or adopted by them.

#### **For the purposes of this document we use the following 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 who publish their own material.

**Connectivity Providers:** Companies that provide access to the internet.

## Good Practice Model for providers of Web Based Services

**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 encourage 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.

## 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, explicit sexual or 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 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<sup>8</sup>.

## Web Good Practice Model

### 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, who the content is for, so as to avoid offending users or taking them by surprise.
2. **Websites specifically aimed at 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.
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 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<sup>9</sup>.

<sup>8</sup> Information Commissioner, [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)

<sup>9</sup> Information Commissioner, [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)

## Good Practice Model for providers of Web Based Services

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.

### **Advice from the Information Commissioner is as follows.**

"The Act does not lay down a precise age at which a child can act in his/her own right and the Commissioner does not consider it is valid to try and do so. Much depends on the capacity of the child and the complexity of the proposition that is being put to him/her. As a general rule the Commissioner considers the standard adopted by Trust UK ([www.trustuk.org.uk](http://www.trustuk.org.uk)) in its accreditation criteria to be a reasonable one. This is that:

'Personal data must only be collected from children with the explicit and verifiable consent of the child's parent/guardian unless that child is aged 12 years or over, the information collected is restricted to that necessary to enable the child to be sent further but limited on-line communications and it is clear that the child understands what is involved.'

The above standard is based on the definition of a child as a person aged 16 years or under.

There are certain practices that, if adopted, are likely to breach the requirements of the Act. These include collecting personal data relating to other people (for example parents) from children and enticing children to divulge personal data with the prospect of a game prize or similar inducement. If personal data collected from children are to be disclosed or transferred to third parties this should not take place without the explicit and verifiable consent of the child's parent/guardian unless it can be demonstrated that the child really appreciates what is going on and the consequences of his or her actions.

Similarly, where a website operator wishes to publish personal data relating to a child on the internet the verifiable consent of the child's parent/guardian should usually be obtained. Whether it is necessary to seek the parent or guardian's consent to publication, rather than that of the child, will again depend on the circumstances, in particular the age of the child, and whether or not the data controller can be certain that the child fully understands the implications of making their information available on the internet.

Where parental consent is required the website operator must have some way of verifying that this has been given. It will not usually be sufficient to simply ask children to confirm that their parents have agreed by means of a mouse click. It will in all likelihood be necessary to revert to postal communication. If parental consent is the required standard but the website operator concludes that the effort in verifying the consent is disproportionate, the proposed marketing activity or other course of action should not be pursued."

**7. The Advertising Standards Authority has specific rules about children that apply online as well as offline. For example:**

- advertisements and promotions addressed to or featuring children should contain nothing that is likely to result in their physical, mental or moral harm, and
- advertisements and promotions addressed to, or featuring children should not exploit their credulity, loyalty, vulnerability or lack of experience:<sup>10</sup>

<sup>10</sup> [www.asa.org.uk/the\\_codes/show\\_codes.asp?page\\_no=43](http://www.asa.org.uk/the_codes/show_codes.asp?page_no=43)

## Good Practice Model for providers of Web Based Services

8. **Content providers are encouraged to consider self-labelling** (i.e. describing the content of their site) with PICS compatible systems such as ICRA's system. It is acknowledged such systems need further development but they can play an important part in dealing with content issues<sup>11</sup>.

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

10. **Websites should be careful about including photos**, contact or other details, which together could serve to make children identifiable and contactable<sup>12</sup>.

11. **Providers of content aimed at children** should also provide a contact address for complaints and act upon them as appropriate.

### *Third party content*

A number of content providers allow web users to add material to their web site, 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 third parties** 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 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;

<sup>11</sup> PICS <http://www.w3.org/PICS/>. ICRA [www.icra.org](http://www.icra.org)

<sup>12</sup> The Department for Education and Skills offer some advice here with regard to practice in this area, particularly for schools, but which is relevant to others – see <http://safety.ngfl.gov.uk/?INDEX=ALL>.

### *Message and bulletin boards*

- that message and bulletin boards aimed at 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<sup>13</sup>:

- 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;
- 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 children offering search engine facilities should consider providing and promoting "child friendly" searching.

<sup>13</sup> See good practice documents on Chat and Instant Messenger for further details on good practice with interactive services.

### *Providers of Adult Content*

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

- 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/ URL's.

## 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 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 on-line behaviour, and that unacceptable behaviour will 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.

## Good Practice Model for providers of Web Based Services

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 inform users** they can make a report to the IWF about pornographic or racist material they believe may be illegal. They may also wish to provide a hyperlink to the IWF site<sup>14</sup>.

### 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.

2. **Terms of Service should make clear the limits** of acceptable on-line 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 such as ICRA's. It is acknowledged such systems need further development but they can play an important part in dealing with content issues<sup>15</sup>.

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

<sup>14</sup> PICS [www.iwf.org.uk](http://www.iwf.org.uk)

<sup>15</sup> PICS <http://www.w3.org/PICS/> ICRA [www.icra.org](http://www.icra.org)

## List of Members of Sub Group F

### (Child Protection Measures)

Lynda Jackson (Home Office) – Chair

Chris Atkinson (NSPCC)

Charlotte Aynsley (BECTA)

Kevin Baigent (V21)

Rachel Basger (World OnLine)

Kiran Bhanaut (DfES)

Robin Blake (ITC)

John Carr (NCH)

Julian Coles (BBC Online)

Rachel O'Connell (University of Central Lancashire)

Ann Cooper (Wired Patrol)

Ruth Dixon (Police Training)

Donald Findlater (Wolvercote Clinic)

Stephanie Harris (ISPA)

Sam Howells (Dubit)

Malcolm Huddy (Campaign against Censorship)

George Kidd (ICSTIS)

Aimery Martin (SurfControl)

Shereen Meharg (Microsoft)

Annie Mullins (Yahoo!)

Ute Navidi (ChildLine)

Roland Perry (LINX)

Priscilla Patten (Home Office)

Stephen Quick (Met Police)

Camille de Stempel (AOL)

Catherine White (Supanet)

David Ware (Home Office)

Nigel Williams (Childnet Int.)

Andrea Wills (BBC OnLine)

## Project Teams

### Instant Messaging

Annie Mullins (Yahoo!) – Chair

Chris Atkinson (NSPCC)

Rachel O'Connell (University of Central Lancashire)

Shereen Meharg (Microsoft)

David Ware (Home Office)

Nigel Williams (Childnet Int.)

### The Web (1)

Ruth Dixon (internet Watch Foundation) – Chair

John Carr (NCH)

Alice Morrison (Supanet/Time)

Camille de Stempel (AOL)

Andrea Wills (BBC OnLine)

### The Web (2)

Annie Mullins (Yahoo!) – Chair

Chris Atkinson (NSPCC)

Kevin Baigent (V21)

Julian Coles (BBC Online)

Will Gardner (Childnet Int)

Cathy Gerosa (ICSTIS)

Mark Gracey (Thus)

Ute Navidi (ChildLine)Camille de Stempel (AOL)

David Ware (Home Office)

### SPAM

Roland Perry (LINX) – Chair

Richard Clayton (Thus)

Stephanie Harris (ISPA)

Malcolm Huddy (Campaign Against Censorship)

Aimery Martin (Surf Control)

Ute Navidi (ChildLine)

