Ofcom's Submission to the Byron Review

Annex 2: Current tools and approaches to protecting children from harmful content online

Submission date:
30 November 2007

Contents

Section 1

Introduction

In this paper we consider the challenges of internet regulation in general; review the approaches currently adopted in the UK to protect children from potentially harmful content when online; and summarise the key controls and tools available at each point in the value chain. We also describe briefly the distinct approaches taken to managing the availability of illegal content online

Section 2

The challenge of protecting children online

2.1 General approaches to internet regulation

Before reviewing the approaches applied to protecting children from potential harm online, it is worth placing this analysis in the context of the broader debate about internet regulation.

The global, dynamic nature of the internet and the variety of services, applications and content types it offers sets it apart from other media to which regulation has traditionally been applied. Unsurprisingly, then, the appropriateness and feasibility of traditional approaches to regulation have been questioned ever since the internet came into being. Two questions are central to these debates: whether the internet should be regulated, and whether it can be regulated.

Should the internet be regulated – the views

Views vary widely on whether it is right to control the internet. At one end of the spectrum is the argument that no regulation should even be attempted, as a matter of principle. This position is most famously expressed in John Perry Barlow's 1996 "Declaration of Independence of Cyberspace[1] " which argues for the freedom of the internet from any government control. However, the recent net neutrality debate in the US has turned the argument around, with proponents of net neutrality arguing for government intervention as a means of ensuring the ongoing freedom of the internet[2].

Another argument against regulating the internet in principle is that, in contrast to traditional broadcast content, it requires users actively to seek out and choose the content they access. This is different to traditional television content, which reaches large audiences simultaneously and where the viewer has more limited choice over content once the television is switched on. (This is covered in detail in Annex 3)

At the other end of this spectrum is the argument that the internet has in fact never been unregulated. Laurence Lessig, for example, suggests that the laws, or social norms, regulating offline activities are replaced online by the software codes which have always formed the basic layer of internet regulation. The internet is, therefore, already governed by software algorithms put in place by the individuals and organisations involved in online activities[3].

Can the internet be regulated – the views

Views on whether the internet can effectively be controlled also vary. Those who argue that it cannot highlight the difficulty of applying regulation, citing a number of practical factors: jurisdictional variations, the rapid pace of change in internet services and architectures, and the challenge of regulating millions of content provision and access points around the world. Others say that it is possible to implement controls, pointing to countries – such as China and Saudi Arabia - which have sought to control the online content available to their citizens

[1] See http://homes.eff.org/~barlow/Declaration-Final.html
[2] See e.g. Sashkin (2006) Failure of imagination: why inaction on net neutrality regulation will result in a defacto legal regime promoting discrimination and consumer harm. Commlaw Conspectus – Journal of Communications Law and Policy, 15 (1) http://commlaw.cua.edu/articles/v15/sashkin.pdf
[3] Lessig (2000) *Code and other laws of cyberspace*. Preview and excerpts available at http://code-is-law.org/

through the use of the law of the land and technical measures. Critics of such country-wide technical solutions have drawn attention to the consequences, including compromised freedom of expression, when such measures are applied.

An example of recent regulatory thinking on the topic is the approach proposed by Elli M.Noam[4]. Noam acknowledges both the difficulty of controlling the internet and the ongoing desire of societies to pursue regulation to achieve social or economic objectives. Noam suggests that in the future regulation will increasingly focus on the "least mobile and least elastic" elements of the value chain, as these are the only parts where controls can be applied by governments and regulators. Rather than regulating electronic content, which is increasingly outside the regulators' control, regulation will be applied to physical assets and/or significant segments of the value chain under the regulators' jurisdiction. Noam argues that, as convergence continues and the internet becomes the primary platform for most media uses, regulators will have to turn their attention to ISPs in order to secure content policy objectives – because ISPs are the only players within jurisdiction.

The suggestion that securing content goals might be secured through ISP regulation has excited a great deal of opposition in policy debates. As we discuss below, the basic framework for telecommunications regulation in the EU confers particular protection on industry actors who are 'mere conduits'. A 'mere conduit' cannot be held responsible for the content passing over its networks.

This protection is based on a fundamental distinction between the providers of connectivity like ISPs and of content on sites like Yahoo! or the BBC, The role of the ISP is to carry digital packets, not to manage content services, and so it does not make sense to make them responsible for the content services which the packets they carry make up. An ISP is in some ways like a provider of traditional telephony – responsible for connecting people or businesses, but not for the content of their conversations or other communications. More formally, ISPs are not direct economic participants in the content markets which they enable: they are compensated for carrying data packets, whether those packets will make up an email, a television programme or some high-value financial market information. These considerations mean that direct regulation of ISPs is unlikely to be an appropriate or effective means through which to secure content goals.

2.2 The challenges of protecting children from harmful online content

Compared to linear broadcasting, there are a number of challenges in protecting children from harmful content online:

- **The global nature of content on the internet:** this relates not only to issues of scale and coordination, but also to cultural differences - what is considered harmful in one country may be acceptable in another. This issue is not unique to internet content, but while broadcast television standards can be effectively applied in one territory, this is not the case online, where most content is global and can be accessed anywhere in the world.

- **The proliferation of user-generated versus commercially-produced content**: As opposed to traditional television, where content producers and/or broadcasters are relatively few and usually easily identified, anyone can publish online using simple technologies and software. Tools for producing and circulating different kinds of content – text, images and videos – are widely available and affordable to many

[4] Eli M. Noam is Professor of Economics and Finance at the Columbia University Business School since 1976. For an overview of Noam's approach see "Why TV regulation will become telecom regulation" in *Communications: The Next Decade* (Ofcom, 2006)

people around the world. For example, producing and sharing a personal video with friends and family was, in the past, a considerable and a rather expensive task. Today, anyone can record a video on their mobile handset, and share it with a global audience of over a billion[5] users within minutes.

- As a result, the amount of potentially harmful material is significantly above what has ever been available via traditional media. For example, the European internet hotline association, INHOPE, processed 400,000 reports about illegal or harmful content in 2006, representing 33,000 reports per month. These are likely to reflect only a fraction of such content available online, as very few users report illegal or harmful content when they encounter it[6]. An extensive quantitative study carried out in the US in 2006 estimated that 1.1% of sites catalogued in Google and MSN contain sexually explicit content[7]. This suggests that there were 264 million such pages available online at the time.

- **The way in which the internet is used by children.** Another issue in relation to online content is the greater difficulty of managing children's use of the internet, both fixed and mobile, compared to traditional media. The internet is pervasive and accessible from a variety of locations such as home, school, internet cafés – or anywhere at all using internet-enabled mobile handsets. Potentially harmful content is present online constantly rather than during defined time periods as is the case with broadcast television. In addition, the internet tends to be an individual consumer experience compared to television, which is often a shared experience.

2.3 Controlling potentially harmful content at various points in the value chain

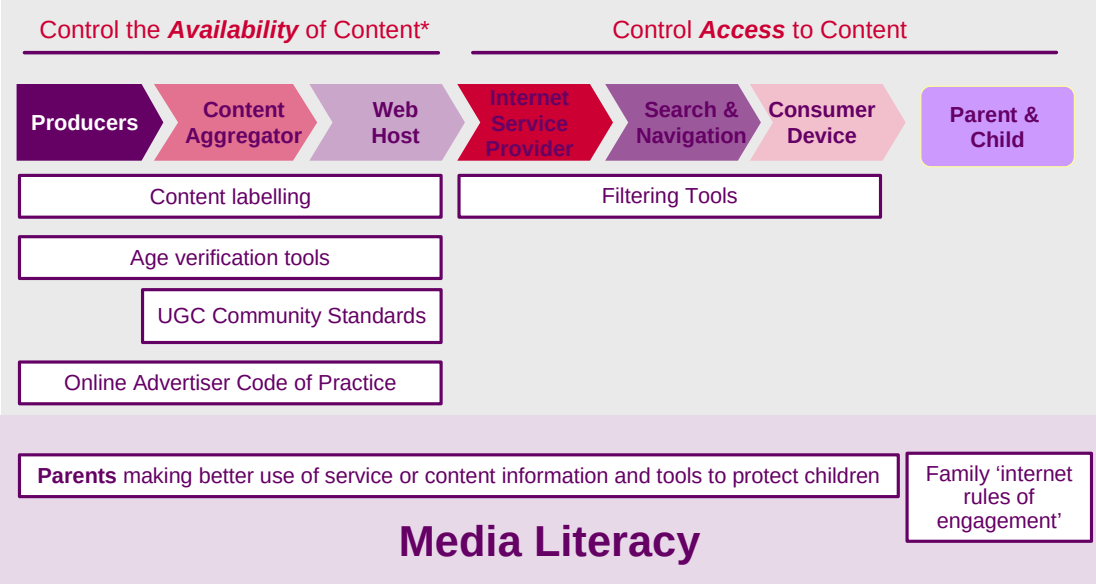
Controls designed to limit children's access to potentially harmful content online can be put in place at different points of the value chain, as shown in Figure 1 below. There are two types of control activities:

- Activities aimed at controlling the *availability* of potentially harmful content; and

- Activities aimed at controlling children's *access* to such content.

5 http://www.internetworldstats.com/stats.htm
6 According to INHOPE, only around 4% of EU population is aware of possibility to report such content to a hotline.
7 Webroot (2007) http://www.webroot.com/pdf/Webroot_SoIS_Q0207.pdf [accessed 19/10/07]

Figure 1: Controls applicable at different points of the value chain



2.3.1 Content producers

Producers of illegal content are a target of law enforcement authorities. In the UK the police investigate incidents of suspected illegal online content and other activities. They take direct action in relation to UK-based producers, and co-ordinate with other countries' authorities to deal with overseas-based criminal content producers.

Producers of legal content that is potentially harmful for children can label it to enable filtering software and search tools to prevent children accessing it. There is no legislation requiring producers to label content in the UK, although self-regulatory arrangements (such as the mobile operators' code of practice) may apply to specific players in the value chain. We discuss the current labelling systems in Section 2.5 below.

2.3.2 Content aggregators

As discussed in Annex 1, the broad category of content aggregators includes a variety of players, including those maintaining their own portals as well as those supplying content further down the value chain.

Content aggregators apply a variety of solutions, including:

- defining and monitoring codes for aggregated content – for example, requiring third-party providers to label content;
- classifying content to indicate that which is unsuitable for children and limiting the types of third-party content they aggregate;
- implementing age verification mechanisms for specific content on their portals, or for overall access to their portals;
- applying filtering, both of their own portal material and/or wider internet content, in search facilities provided on aggregator websites;
- compiling child-friendly versions of their portals, giving access only to content appropriate for children; and

- providing information on safe internet use for children and parents.

2.3.3 Web hosts

Web hosts remove illegal or defamatory content when alerted to it, for example by the Internet Watch Foundation (IWF)[8] or the law enforcement authorities.

Web hosts may also voluntarily remove harmful content when requested, subject to the terms on which hosting services are provided. This voluntary role is of particular importance when we consider the providers of user-generated content hosting services, among which the most popular is YouTube.

Therefore, while web hosts play a crucial role in reducing the availability of illegal or potentially harmful content, they do not play a role in identifying such content. Hosts, like ISPs, are protected under telecommunications regulation from any legal requirement to monitor the content they are hosting (see Section 2.4 below).

2.3.4 ISPs

ISPs serve as the gateway to the internet – both for consumers who sign up to their services, and for internet traffic that goes though the ISP infrastructure. ISPs can play a number of roles in controlling the availability of, and access to, potentially harmful content:

- blocking illegal content, using a list of websites known to supply, or suspected of supplying, illegal content;
- offering network-layer filtering services to parents which control access to potentially harmful content;
- offering filtering software packages; either free as part of the internet package, or at additional charge; and
- providing information on safe use of the internet for parents and children.

2.3.5 Search and navigation

Search and directory providers can play a variety of roles, both in reducing the availability of, and controlling access to, potentially harmful content:

- removing links to illegal content when alerted by national law enforcement authorities;
- offering the option of filtered of search results; and
- providing child-friendly search and directory facilities.

8 The IWF is a regulatory body working to minimise the availability of illegal content online

2.3.6 Consumer devices

Consumer devices – such as PCs and laptops – are the point in the value chain where filtering software can be installed and used by consumers.

In addition, operating system software may give the consumer options for controlling access for potentially harmful content. Such features are now available for major operating systems including Microsoft Vista and Apple OS X. (See Section 2.6 for more detail)

2.3.7 Parents and children

Parents have a key role in protecting their children from coming across potentially harmful content. They set and police rules for their children's use of the internet, both in terms of content accessed and time spent online. Parents have a key educational role to play in enabling children to use the internet safely.

Both parents and children can report illegal content to law enforcement authorities. They can also alert other internet value chain players to potentially harmful content that breaks their guidelines (such as terms and conditions of use, classification rules). Filtering systems often have a feedback mechanism whereby parents and children can report mis-categorised websites.

2.3.8 Internet management

In addition to the value chain elements above, there is a layer of activity which supports the operation of the internet, by managing the underlying technologies such as protocols and addressing systems, through bodies like ICANN (the Internet Corporation for Assigned Names and Numbers). Most activity taking place at this layer is not directly related to controlling the availability of content; however, there are two instances where there is a direct relationship:

Management of domain names: Designating specific domain names for different types of content can simplify the introduction of blocking and labelling measures. A relevant example here is a proposal for .xxx domain names to be used by providers of pornographic content. The proposals were first put forward by ICM Registry in 2000. Proponents of the .xxx domain suggest that this would enable efficient and simple blocking of pornographic content by filtering tools. The proposals were rejected by ICANN in 2005 and again in 2007, most importantly because ICANN felt that the proposals could mean "*ICANN would be forced to assume an ongoing management and oversight role regarding Internet content, which is inconsistent with its technical mandate*[9]"

IP address geo-location: IP addresses are typically allocated on a country-wide geographic basis to individual ISPs. As a result it is possible for service providers to block services to, or from, particular parts of the world, or from specific ISPs. This technique can also be used to infer the local time, and so can be used to enable time-based blocking, e.g. of adult content. It is worth noting that some older IP address allocations pre-date the geographic arrangement, so such blocking may not be perfect.

9 Adopted Resolutions from ICANN Board Meeting, 30 March 2007. http://www.icann.org/minutes/resolutions-30mar07.htm#_Toc36876524

Both of these can contribute to the effectiveness of filtering activity, but neither of these is a discrete form of intervention, so we do not consider them further below.

2.4 The legal framework

This section outlines the most important aspects of the legal framework relating to online content provision and illegal content. (We discuss the handling of illegal content in Section 2.11 below; however, aspects of the legal framework are also important in considering harmful but legal content, the main focus of the Byron Review)

In general, the originators of online content (e.g. content producers and aggregators) have the same broad liabilities as do print media publishers. However, the impact of these liabilities on content providers' behaviour is constrained by of national jurisdictions – providers outside the UK's reach will not need to comply with UK rules. Furthermore, there are a number of important limitations on the liabilities of web hosts and of internet service providers, in the context of the Electronic Commerce Directive (the "Directive")[10] as implemented in the UK in the Electronic Commerce (EC Directive) Regulations 2002 (the "Regulations"). Specifically, the framework covers the providers of "information society services", defined as any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service". This covers online services provided for remuneration, and extends to services which are not remunerated by those who receive them, such as those offering online information or content, or those providing search, access and retrieval of data.

2.4.1 "Mere conduits"

Internet access providers (ISPs) will often have a protected status under the Directive. This is because they are likely to be what the Directive describes as "mere conduits".[11] Where they do not initiate the transmission of content, select the receiver of the transmission, or select or modify the content transmitted, they do not have legal responsibility where that content is unlawful.

The Directive also prevents Member States, including the UK, from imposing general obligations on service providers (including mere conduits), to monitor the content they transmit or store or to actively seek facts or circumstances regarding illegal activity.

2.4.2 Hosts' legal status

Those that provide an information society service consisting of "the storage of information provided by the recipient of the service" also have protection from liability. Hosts are not liable in relation to the illegal third party content they host, provided that they do not have "actual[12] knowledge" of unlawful activity or information, or upon obtaining such knowledge or awareness, they act expeditiously to remove or disable access (i.e. to remove the content).

10 Directive 2000/31/EC
11 Defined in the Directive as where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network.
12 The Regulations define what is meant by "actual knowledge" and suggests that a court should have regard whether a service provider has received notice of the unlawful information in question (in accordance with information to be provided under the Regulations to an end-user) and the extent to

Secondly, as for ISPs, the UK is prevented from imposing a general obligation on intermediaries, including hosts of third party content, to monitor information which they transmit or store, or a general obligation actively to seek the facts or circumstances indicating illegal activity. This means that it would not be possible under current UK and EU legislation to require hosts to take responsibility for monitoring the content they host.

2.5 Internet content labelling

Content labelling is the process of attaching descriptive information to web pages or other content assets. This labelling data can be used either directly by audiences to determine what content to access; or indirectly by filtering tools, search engines and online directories to classify content.

Accurate content labels can be used to manage access to potentially harmful or inappropriate content – for example by controlling children's access. Content labelled pornographic or violent can be eliminated from search results or blocked by a filtering tool. However, the extent of adoption of labelling which would enable such content filtering is currently very low.

Labelling of internet websites: ICRA

The Internet Content Rating Association (ICRA) is an international, non-profit-making organization set up by the Family Online Safety Institute (FOSI). It has developed a content description system in which the labels applied by content providers are attached to the websites as an information file. The information contained in the labels can then be used by filtering tools to determine the sites to which access should be blocked, based on the filtering tool's specifications. ICRA itself provides a free filtering tool, *ICRAplus*, which mirrors its content labelling categories.

Figure 2

ICRA labelling system

The system allows content producers to self-label the material published online. The classification was first introduced in 2000, and designed to provide a reasonable consistency across different cultures and languages. This includes categories of potentially harmful material, such as:

- Nudity
- Sexual material
- Violence
- Language that may be inappropriate for children
- Depiction of potentially harmful activities such as use of tobacco or weapons

Content can also be classified as user-generated content; in addition contextual information about the material presented (such as news, or artistic content) can also be applied. Content publishers can also create and assign their own labels if required.

which it includes the sender's name and address, details of the location of the information and details of its unlawful nature.

As ICRA itself acknowledges, while the system aims to provide objective descriptions, some subjectivity and ambiguity in self-labelling is inevitable[13].

ICRA is supported by the European Union's Internet Action Plan and various trusts and foundations. It works to continually improve and extend the application of content labelling. A recent development in this area is the EU-funded Quatro project, which will integrate content labels with quality and trust marks. ICRA also intends to launch a service to verify the accuracy of ICRA labels and to provide this information to third party tools and services, such as search engines.

Despite the wide availability of easy-to-use labelling tools, the application of internet website self-labelling using any kind of common framework is negligible. A number of factors contribute to this. First, there is a lack of support for labelling within the most popular software packages for creating web content. Second, the incentives to label for content producers are generally low, unless requested by content aggregators as part of commercial agreements or embedded in the aggregators' codes of practice.

According to the expert panel report evaluating the activities of the EU Safer Internet Action Plan in 2003-2004, there is a general reluctance among internet content producers to apply labels, especially for establishing blacklists. The report concluded that "voluntary self-labelling cannot provide a solution to tackle the problem of unlabelled web pages, except if labelling becomes compulsory".

However, it should be noted that because the internet is a pull environment, all content providers have strong incentives to provide accurate information about the characteristics of the content they are offering, to enable interested audiences to find it: unless a user knows something about what to expect, there is no reason to look at a given piece of content. The gap is in the application of common labelling, which could be used to manage or control access to specific types of content.

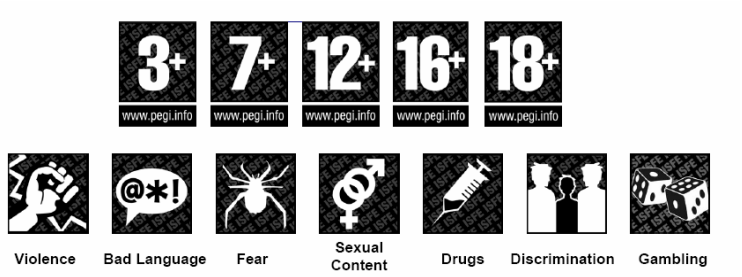
Rating of online games: PEGI Online

PEGI Online is a European classification system for online games, developed by the Interactive Software Federation of Europe (ISFE). The ISFE was established in 1998 to represent the interests of the interactive software sector and is open to any company within the sector in the 27 member states plus Norway, Iceland, Switzerland and Liechtenstein. Thirteen major publishers of interactive software and eleven interactive software trade associations throughout Europe have joined ISFE.

The ISFE launched the Pan-European Game Information (PEGI) in 2003 as a self-regulating, pan-European rating system for computer games. The rating system comprises two separate but complementary elements: the first is an age rating, with age bands of 3+, 7+, 12+, 16+, and 18+. The second element is a set of game descriptors, such as "bad language", "drugs" and "fear". As of March 2007, 6,697 games had been rated by PEGI.

[13] http://www.icra.org/label/generator/ [accessed 29/10/07]

Figure 3: PEGI labels



PEGI Online was developed and launched in 2006 with the support of the European Commission. The system is based on four cornerstones:

- the PEGI Online Safety Code and Framework Contract;
- the PEGI Online Logo, to be displayed by licence holders;
- a dedicated website for applicants and for the general public; and
- an independent administration, advice and dispute settlement process.

The licence to display the PEGI Online Logo is granted by the PEGI Online Administrator to any online gameplay service provider that meets the requirements set out in the PEGI Online Safety Code (POSC). The code was developed to provide a minimum level of protection to young people in the online gaming environment. The requirements include the obligation to keep the website free from illegal and offensive content created by users, and any undesirable links, as well as measures for the protection of young people and their privacy when engaging in online game playing.

The PEGI Online Logo will appear on the packaging of games sold on a CD/DVD, and on the game website itself. The logo will show whether the game can be played online, and also whether the particular game or site is under the control of an operator that cares about protecting young people.

Figure 4

PEGI Online Safety Code – summary

Age-rated game content: Only game content that has been appropriately rated under the regular PEGI system or another recognized European system, such as that operated by the BBFC in the UK or the USK in Germany, will be included on a site.

Appropriate reporting mechanisms

Appropriate mechanisms will be in place to allow game players to report the existence of undesirable content on any related websites.

Removal of inappropriate content

Licence holders will use their best endeavours to ensure that online services under their control are kept free of content which is illegal, offensive, racist, degrading, corrupting, threatening, obscene or which might permanently impair the development of young people.

A coherent privacy policy

Any PEGI Online licence holder collecting personal information from subscribers will maintain an effective and coherent privacy policy in accordance with European Union and national Data Protection laws.

Community standards for online subscribers

PEGI Online licence holders will prohibit subscribers from introducing content or indulging in online behaviour which is illegal, offensive, racist, degrading, corrupting, threatening, obscene or which might permanently impair the development of young people.

A responsible advertisement policy

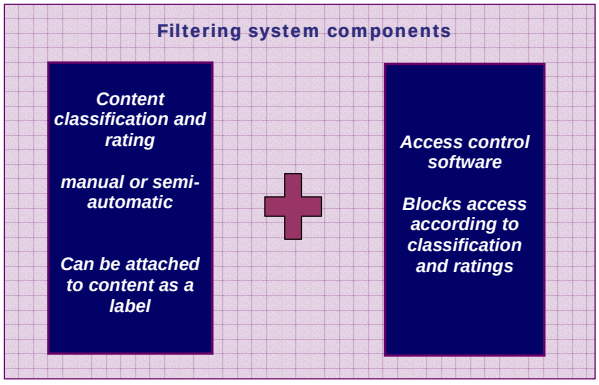
- all advertisements will accurately reflect the nature and content of the product represented and wherever reasonably practicable the rating issued
- all advertisements shall be created with a sense of responsibility towards the public
- no advertisement shall contain any content that is likely to cause serious or widespread offence
- advertising for products rated 16+ or 18+ shall not be specifically targeted towards those who are younger
- ancillary or separate products that are being sold or promoted in association with a core product must be appropriate for the audience for which the core product is intended
- licence holders should inform the public by means of a general statement of the existence of sponsorships and/or the existence of ‘product placements’ associated with any online service

2.6 Filtering tools

2.6.1 Filtering tools to block access to potentially harmful content

The objective of a filtering system is to block access to websites and internet services offering illegal or potentially harmful materials. There are two parts to a filtering system: the identification of unacceptable content; and the subsequent process of blocking access to it.

Figure 5 Filtering system components



To be able to provide appropriate levels of web filtering, content must be classified and rated. Typical categories include sexual activity; nudity; violence; drug-related; race hate; gambling; alcohol; and tobacco.

Many filtering tools offer a choice of levels according to child age ranges. For example, AOL's parental control tool distinguishes between three child categories and an adult category[14]:

- **Kid (12 and under):** Allows access to age-appropriate features and content through AOL's Kids Channel and the rest of the internet (when accessed through AOL). Premium services and instant messages are blocked. Limited email, instant messaging and monitored children's chat.
- **Young Teen (13-15):** Allows access to age-appropriate interactive features and information on AOL and the rest of the internet (when accessed through AOL). Premium services and instant messages, as well as private and member chat rooms, are blocked.
- **Mature Teen (16-17):** Allows the most freedom of all the children's categories. Gives access to most interactive features and information on AOL and the rest of the internet (when accessed through AOL). Web sites with explicitly mature content are blocked.
- **General (18 and older):** Allows full access to all features and content on AOL and the rest of the internet.

14 http://help.aol.co.uk/

As a general principle the threshold of acceptability of content varies according to the ages of children and their families' cultural backgrounds. Many filtering solutions are designed to be flexible and allow parents to configure the types of content that should be blocked.

2.6.2 Classification techniques

Classification information can be attached to the content by its creator in the form of a label, as discussed in Section 2.4. Alternatively, it can be maintained in a third party database which is made available to access control systems (typically via file download over the internet).

Blocking lists, pass lists and labelling

Two types of list are used by filtering tools:

- A blocking list is used to identify the locations of unacceptable content and consists of sets of web addresses (URLs) and server IP addresses. Blocking lists typically assign content assets to different categories according to their editorial characteristics. This enables filtering systems to provide different levels of filtering appropriate to different age groups and cultural sensitivities.

- Pass lists are the opposite of blocking lists - they list those locations where the content is known to be 'safe'. They are particularly useful for controlling the access of younger children who need a higher level of protection and are less likely to want to surf the internet in the same way as older children and adults.

List generation is a complex and time-consuming activity for the providers of filtering services, although user feedback and automatic tools can be used to help maintain and extend lists. Sites carrying rapidly-updated user-generated content such as videos and photographs are in practice impossible to rate accurately using automatic tools.

Accurate content labels also help filtering tools to classify content. However, only a very small proportion of websites are labelled in a way that allows easy classification.

2.6.3 Automatic content analysis

Automatic analysis is a technique for controlling access to text-based content such as web pages, Word and pdf files. These types of content can be processed without significant delay as they load, providing protection against content which has not already been classified by the filtering provider. Filters typically look for keywords, phrases and other indicators such as the type of language and the text-to-image ratio. Labels and metadata can be useful in refining automatic filtering.

Video materials present a particular challenge for automatic filtering as they are sequences of rapidly changing images together with audio:

- Video is conveyed as a compressed file which has had all the redundant parts of the image and sound removed. It can be analysed only if the tool has access to the correct decompression software (codec). Without this the file cannot be reconstructed into a video signal and is seen only as a sequence of meaningless numbers.

- Digital Rights Management (DRM), which controls who has the right to unencrypt audio-visual content, is a major issue for commercial content as it can block

reconstruction of the video and therefore any analysis of it.

- While 'static' content can be analysed in advance and added to a blocking list if necessary, accurate labelling, metadata or linking text may be essential for adequate control of access to rapidly-updated sites, such as those carrying user-generated content.

The processing power required to analyse a video file is orders of magnitude greater than to search a text-based document. Image analysis tools are currently at an early stage and perform best when combined with analysis of linking text or metadata.

Websites are not the only source of content – potentially harmful content is also widely available via newsgroups (Usenet) and peer-to-peer (P2P) file-sharing networks. Content can also be exchanged via FTP, instant messaging and email. Because of this, internet filtering systems typically also attempt to manage access to these services - with varying degrees of success and functionality.

Figure 6 below summarises the advantages and disadvantages associated with each of these classification techniques.

Figure 6: Strengths and weaknesses of classification techniques

Technique		Description	Advantages	Disadvantages	Comments
List-based	**Pass lists (walled gardens)**	Users can only view sites from a defined list. When a site is requested, it can only be viewed if it is on the list. Can be used by a PC filtering program, or a 'walled garden' ISP-filtered service.	▪ Safe and reliable ▪ Simple and fast ▪ Low processing requirement	▪ Over-blocking ▪ Lists of 'allowed' sites are subjective ▪ Hard for parents to build a large list of their own	▪ Suitable for young children, but too limited for older children and adults
	Blocking lists	Users cannot view sites included in the blocking list. Can be used with a client PC application (included with application and/or supplemented by users), or an ISP- layer filter.	▪ Simple and fast ▪ Limited over-blocking if list is accurate ▪ Can classify sites into wide range of categories ▪ Low processing power requirements	▪ Under-blocking ▪ Changing and new URLs and proxy servers not blocked ▪ Site classification can be subjective ▪ Very poor under-blocking ▪ Manual classification of sites is very labour intensive	▪ Historically the most common approach used by filtering applications ▪ Today, viewed by major application companies as crude and flawed – and as a partial solution at best
Labelling		Content providers rate their sites using an agreed standard (e.g. ICRA), then browsers (e.g. Internet Explorer) or filtering systems can filter according to parental preferences.	▪ Finest 'granularity' of classification ▪ Highest accuracy of content description ▪ Satisfies most civil liberty objections ▪ Low processing requirement	▪ Used by <0.1% sites ▪ Potential for intentional mislabelling	▪ Ineffective as a standalone filtering solution ▪ Useful adjunct to automatic filtering
Automatic filtering		Software on device or ISP server analyses text for keywords or phrases indicating unsuitable content which is then blocked. May also analyse images or	▪ Can block access to unacceptable content in documents such as emails, Instant Messages, websites not yet categorised.	▪ Needs significant processing power, particularly for images and video, and may slow down web access ▪ Range of recognisable content limited for video and image filtering.	▪ Essential for dealing with rapidly-updated and uncategorised sites ▪ Processing power requirements are not an issue for home PCs but more

	video for indications of unsuitable content.		▪ Video filtering is challenged by the need for a wide range of decoders and digital rights management issues	challenging for mobile and ISP-level filters. ▪ Video filtering is at an early stage

2.6.4 Location of filtering activity

Filtering solutions can be installed either on a consumer device such as a home PC or laptop, or at the network layer by the ISP. Both types of filtering have advantages and disadvantages and are appropriate in different circumstances, as shown in Figure 7 below.

Figure 7

Location	Advantages	Disadvantages
Personal computer or laptop	• Adequate processing power available for advanced techniques • Support for multiple user logons • Able to validate user keyboard input • Cannot be bypassed by use of encrypted connection (VPN) to external gateway • Can be incorporated into anti-virus/spam/spyware package[15]	• Needs to be bought/installed • Can be bypassed by booting from a free operating system disk (e.g. Ubuntu Live) • Can be bypassed by introduction of a new device (e.g. WiFi-connected phone)
ISP	• Cannot be bypassed by booting from an operating system disk • Cannot be bypassed by introduction of a new device • Supports all devices no matter how limited processing power	• Additional cost of processing power for filtering beyond simple lists-based filter • Need for ISP to manage multiple user identities and filtering levels for family members • Alternative ISP may be accessible via modem or neighbour WiFi • Can be bypassed via encrypted connection (VPN) to external gateway[16]

The most common application of filtering is by installing filtering programmes on home PCs or laptops. There are many such programmes available on the UK market, and many ISPs offer free filters as part of the internet connection package.

2.6.5 Effectiveness of filtering tools

Under- and over-blocking
All filtering systems are subject to a degree of under- and over-blocking. There are a number of reasons for this:

- the difficulties of accurate automatic classification;
- content has been mis-classified (often resulting from reliance on automatic tools);
- UK/European content is not identified by a US-based organisation;
- US terms are not recognised in the UK;

15 e.g. McAfee Internet Security Suite
16 e.g. https://stupidcensorship.com (note that this particular site is now blocked by most filters)

- lack of an appeals process; and
- an over-protective approach in some areas.

An EU-funded project, *SIP-Bench*, benchmarks filtering products and in 2006 decided the following error rates were appropriate to gain the top performance rating[17]:

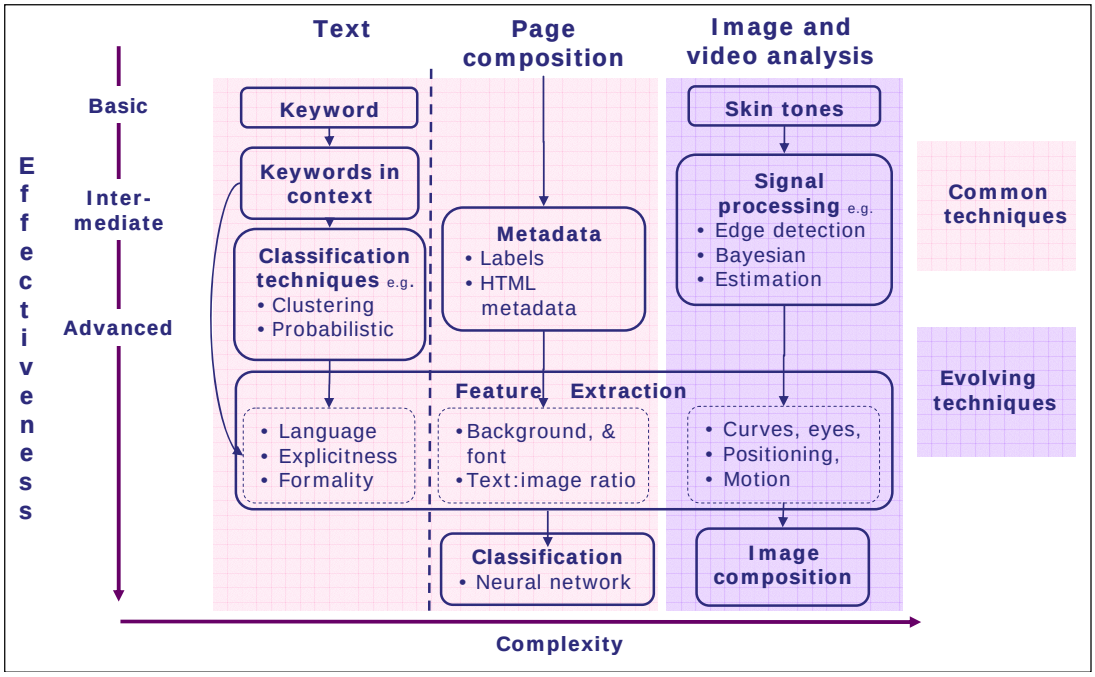
- For 'kids' – blocking 1/8 of 'good' content and passing 1/32 of 'bad' content.
- For 'adolescents' – blocking 1/16 of 'good' content and passing 1/16 of 'bad' content.

A consequence of over-blocking is the need for a parental override, so that access to 'good' content can be enabled. Most access control systems also provide features such as limiting access to chatrooms and instant messaging, and logging attempts to access blocked content.

Filtering systems also need to block access to websites or services such as 'anonymizers[18]', and secure gateways that provide information or facilities to enable children to bypass filters. Although not normally considered part of a content filtering solution, email spam filtering and 'phishing' protection are also relevant. Many spam emails contain pornographic images or 'adult' topics and language. 'Phishing' emails and websites attempt to trick people into giving away personal information. The same techniques can be used to fool people into visiting 'adult' websites.

Newer techniques can reduce under- and over-blocking but require significantly higher processing power. In order to cope with the rapid rate at which new content appears on the internet, new, intelligent features are being incorporated into filtering tools.

Figure 8



Source: Opta

17 Please see http://www.sip-bench.eu/index.html

18 *Anonymiser* is a website that may enable users to access other content in a way which bypasses a PC filter, or may allow anonymous access or online participation

However, to the extent that the determination of “harmfulness” is fundamentally an editorial judgement, in the context of national standards or even individual standards, filters will always involve a degree of inaccuracy, however technically sophisticated they may become.

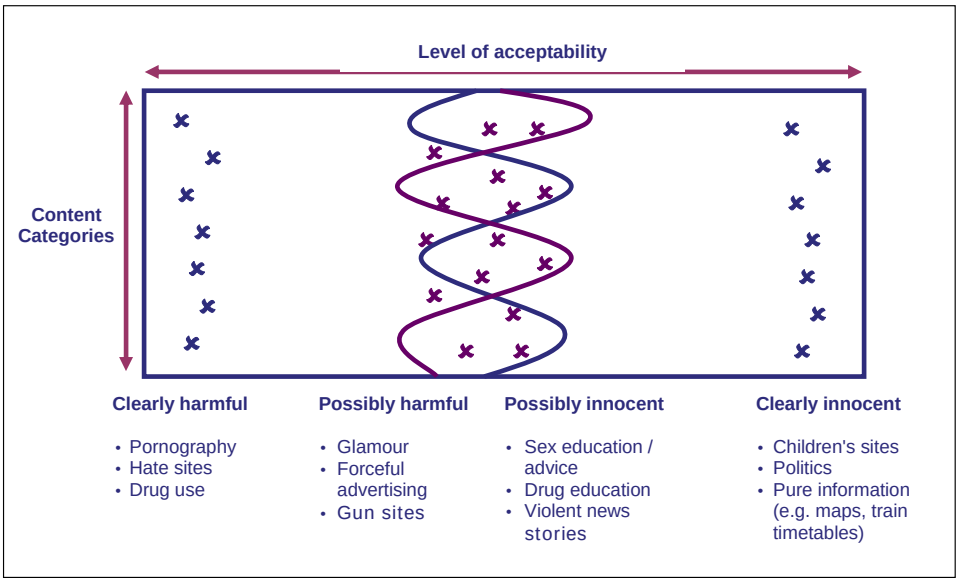
Suitability for home users, and cultural differences

In addition to the general technical challenges described above, there are a number of more nuanced issues, which may prevent filtering tools from being fully effective in all circumstances:

- Some types of content are easy to identify but others require a more subtle approach, to take account of context and cultural sensitivity. Lists created in other countries (typically the US) and for corporate use may be less appropriate for UK households; and UK and US slang can be very different. For example, websites featuring guns are seen as perfectly acceptable in many countries but are frowned upon in the UK.

- The efficiency of filtering depends on the nature of the rating categories and judgements around the innocent / harmful boundary. For example, filtering of the word ‘bomb’ blocked the results of a BBC website search using the terms ‘bomb’ and ‘Bhutto’ (relating to the attempted bombing of Benazir Bhutto on her return to Pakistan in October 2007). The acceptability of content can be highly dependent on context and the subject matter portrayed – as shown in Figure 9 below, a range of content may be considered harmful or innocent.

Figure 9: Continuum of content acceptability



Source: Opta

2.6.6 Testing of filtering products is a challenge

A wide range of home PC filtering products and services are available on the market, with differing levels of performance and functionality. Testing is very difficult to perform adequately, partly due to the rapid rate of change of internet content.

A benchmarking testing project carried out in 2006 by the EU-funded Safer Internet Plus; *SIP-Bench*[19], involved 110 parents and teachers, and a customised lab with its own servers, testing 30 filtering tools in identical circumstances. The study found that filtering tools were able to filter out potentially harmful content without seriously degrading the internet experience of young people. However, of the tools tested, only one achieved the top rating for effectiveness for under-10s. None achieved it for adolescents although two were top-rated for the specific category of pornography.

2.6.7 Filtering tool configuration can be a very complex process

Most filtering tools have a similar level of basic functionality, blocking web access on the basis of lists of acceptable and unacceptable content. Many tools also provide a range of settings to adjust the way the blocking operates, together with a range of additional features and functions, including:

- configuration of blocking options, typically
- 'known good web sites only' (for children)
- selection of blocking categories ('adult', drugs, hate, etc);
- configuration of multiple user accounts with individual filtering levels
- on-the-fly analysis of unrated web pages;
- analysis of text input to search engines and web page forms;
- blocking/analysis of instant messages, chat and email;
- blocking/analysis of email;
- blocking/analysis of FTP file transfer;
- blocking/analysis of peer-to-peer file sharing traffic;
- blocking/analysis of Usenet newsgroup access;
- logging of children's internet activity;
- internet time restrictions; and
- blocking use of computer games; selection of threshold PEGI or BBFC rating.

Most these features are optional – meaning that parents and carers must take some time to familiarise themselves with the options and decide on their appropriateness.

Content filtering is not restricted to dedicated filtering systems. Many internet services and programs include their own facilities, as do the latest computer operating systems from Microsoft and Apple. An unfortunate result of all these options is that there is significant potential for consumer confusion.

[19] www.sip-bench.eu

Figure 10: Selection of blocking categories in Windows Vista

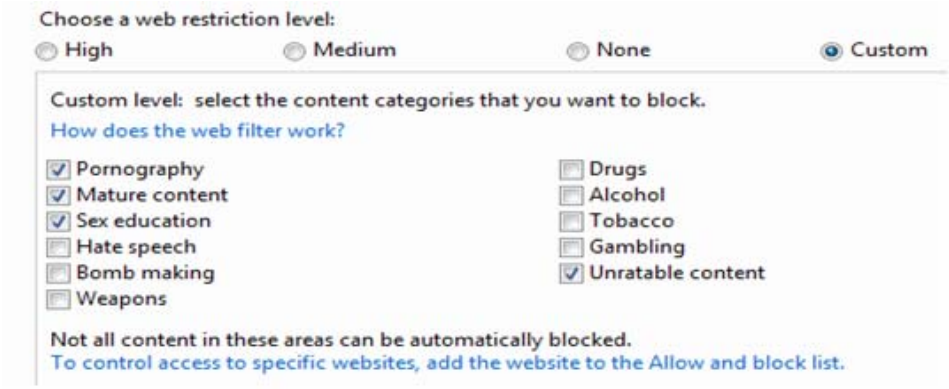


Figure 11: CyberSitter configuration options

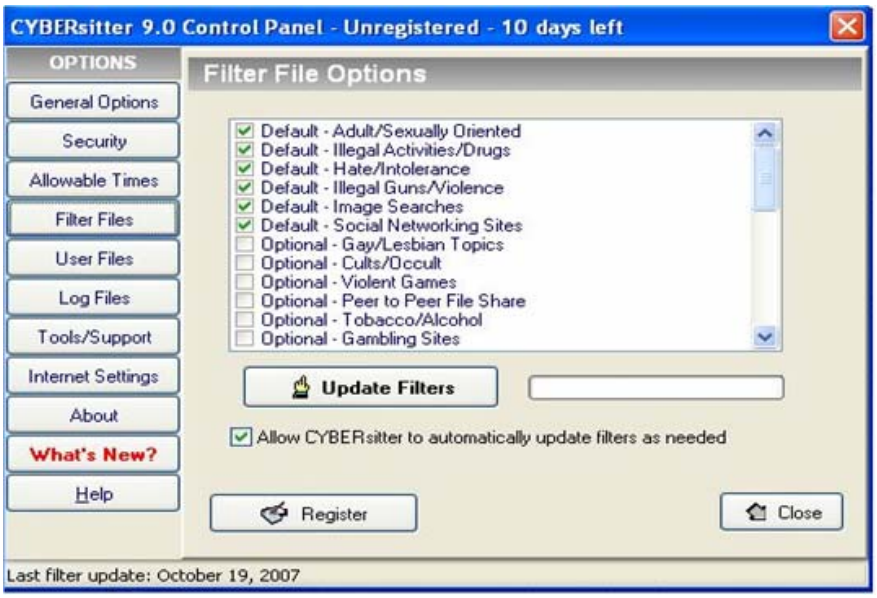


Figure 12: Apple iTunes content filtering options (as used with Apple iPods)

2.6.8 Take-up of filtering tools in the UK

Filtering solutions are widely available in the UK. Parents can acquire filtering software from high-street computer shops or download filtering tools from many online vendors. In addition, many ISPs offer free filtering tools as part of an internet package. Some ISPs offer network layer filtering – for example, AOL's parental control service allows the configuration of network access for multiple users in the home according to different criteria.

The research Ofcom conducted to inform our submission to Byron showed that just over half of parents (54%) with internet access at home say they currently use filtering software[20]. A December 2005 pan-EU survey suggested that use of filtering/blocking tools among parents was significantly higher in the UK than anywhere else in Europe. The level reported in the UK was 46%, compared, for example, to 30% in Germany, 26% in France and an EU average of 28%.[21]

There are no specific requirements in the UK for filters to be used for internet access in public spaces - such as schools and libraries as is the case in some other countries (please see Annex 4). However, Becta (the British Educational Communications and Technology Agency) recommends the use of an accredited BECTA ISP and feeds for libraries are often obtained from Regional Broadband Consortia - most of which are accredited.

2.6.9 BSI Kitemark to build consumer confidence in filtering tools

Following research indicating that consumers were confused about content filtering solutions, Ofcom and the Home Office have jointly sponsored the British Standards Institution (BSI) to work with a number of associated groups to create a specification for 'access control systems for the protection of children online'.

A primary reason for the Home Office and Ofcom to launch the project to create a British Standard for access control software was to encourage the industry to enhance the effectiveness of the existing tools to block access to potentially inappropriate material

The work is intended to result in a range of products that consumers can trust to be effective and also relevant to UK households. It covers products installed locally (i.e. by a parent/carer on a home computer) as well as remotely managed products/services (i.e. those products or services offered by internet service providers or mobile network operators).

The specification sets out the minimum performance requirements for access control systems to obtain conformity certification, including:
ease of installation, configuration and use;

- effectiveness;
- minimum features;
- ease of updating;
- quality of instructions; and

[20] Details in Annex 5
[21] 2005 Eurobarometer survey conducted on behalf of the European Commission among parents with children aged under 15: Special Eurobarometer No 250 – Safer Internet http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm#national_reports

- consumer communications and support.

Work on the Publicly Available Specification, PAS 74, is expected to be complete by the end of 2007.

2.7 Internet gateways: online portals and search engines

We undertook a short survey of rules and practices in relation to harmful content applied by a range of mainstream portals and communities. Please note that while the information was current at the time of conducting the survey (October 2007), these are continually developing services and the details are subject to change. This section summarises the practices put in place by major online portals and search engines. The next section (Section 2.8) looks at social networks, user-generated content sites, gaming sites and peer-to-peer networks.

2.7.1 Online portals

Online portals are access points to information on the internet. They provide a single gateway to information from diverse sources. Their basic function is often a search engine, but portals also offer a much broader range of services including news services, games, shopping, music, and now user-generated content. The four portals we looked at were aol.co.uk, fox.com, lycos.co.uk and yahoo.co.uk.

Content standards and take-down procedures
All these portals had easily accessible terms and conditions documents at the foot of their front page. None of the sites we looked at had summaries of their terms, although Lycos does have a table of contents. Every site lists examples of inappropriate content and behaviour in its terms, with the rider that such examples are not exhaustive. Each list varies but common prohibitions are:

- Obscene, vulgar, pornographic or sexually explicit material.
- Material that infringes copyright.
- Illegal, criminal or fraudulent material or behaviour.
- Dangerous, violent, threatening or abusive material or behaviour.
- Harassment or stalking.

Submitting, downloading or transmitting content (including UGC) of the above types is a breach of the terms of each site. In theory, this is grounds to have an account with the portal terminated, though no site states that this will definitely happen. In addition, all the sites specifically disclaim any duty (though not their right) to pre-screen, to monitor or to take down inappropriate UGC.

The principal means through which portals manage their UGC is through user moderation: members of the audience report concerns to the portal operator. AOL has a ‘notify AOL’ function on all UGC so that users can report inappropriate content. There is also an ‘ignore’ button which lets users automatically block unwanted messages or chat from other users. Yahoo has dedicated ‘report abuse’ forms for each of the different services that it provides.

The other two sites have email addresses for users to report terms violations, though these aren't as well advertised.

All sites state that users might come across inappropriate content while using the portal, and deny responsibility for any of this content produced by third parties or users.

Age restrictions
Yahoo and Fox state in their terms that under-13s are not allowed to set up profiles or to register for fora. They also say that they do not knowingly collect personal information for under-13s. Neither Lycos nor AOL explicitly excludes anyone by age.

Safety guidelines
AOL, Lycos and Yahoo all stress the role of parents in helping to keep their children safe online. They each have a different emphasis: Lycos merely highlights that parents and not Lycos are responsible for the safety of their child, while AOL provides extensive tools and procedures to ensure a family friendly site. Yahoo comes somewhere in between.

AOL encourages parents to take control of their family's internet experience. They allow parents to set different controls for children of different ages. The permissions available are Kids Only (under-12s), Young Teens (13-15), Mature Teens (16-17) and General Access (18+). Access to websites and chatrooms is restricted according to the permission level. Parents can also restrict who their child can email or instant message with and how long their child can spend online. There are also supervised community areas for children and teens, and all AOL chat rooms and message boards have moderators and volunteer 'community leaders'. Moderators can remove messages and moderate chat, while the role of community leaders is to build 'positive' communities. AOL also has detailed community guidelines and a section on 'Netiquette'.

Privacy
All the sites we looked at had privacy policies which set out what the site does with personal data. AOL also has a section with tips to help users keep their personal information safe, while Fox bans the use of personally identifying information on its portal. Yahoo has a 'privacy centre' which a FAQ section on what it does with personal data.

2.7.2 Search engines

Search engines are a central aspect of internet users' experience – the principal means through which audiences choose content. Increasingly search engines incorporate specialised search tools which retrieve images, videos, news or maps. We looked at three of the largest search providers: Google, Yahoo! and Ask.

Content standards and review procedures
Of the three sites we looked at, only Yahoo! has a terms policy accessible from the front page. Google and Ask publish their policies in their 'about' sections. In the case of Ask this is part of a dedicated 'policies' section which includes its privacy and editorial policies.[22]

The three sites clearly state that responsibility for content lies with the originator of the content. They accept no duty to pre-screen, filter or review content on their services, although they reserve the right to do so. Each site warns users in its terms that they may be exposed to offensive content. All three have lists of content that are deemed to be unacceptable, and warnings that those providing this type of content may be blocked from search listings.

Ask in particular has a dedicated editorial policy, detailing the way it generates its search results and how it deals with issues such as adult content. It does not habitually block adult content, but it does display a warning page if it detects that adult sites are included in the search results.

Safety guidelines
Yahoo! publishes a set of parents' guidelines which give advice about keeping children safe online. It suggests that families draw up a 'family pledge' about conduct online, and even provides a sample pledge[23]. Ask has a 'Use of Site by Children' section in its terms and conditions which details parents' responsibility for their children's safety online. It also has guidelines for all downloadable software available from Ask.com, and it requires all advertisers to abide by ASA guidelines on ad content.

Search and filtering
All three sites provide free filters to help manage access to potentially harmful content. Google, the market-leading provider of web search has a '*Safesearch*' feature which has three settings: 'off'; 'moderate' (images are filtered but not text search results); and strict (both images and text are filtered.

Similarly, Yahoo's filter can be set so that text, video and images are filtered or just video and images. Ask has a more simple filter, allowing all results to be screened for adult content), but even with this tool off, Ask warns users when adult content is returned

2.8 Online communities

2.8.1 User-generated content hosts and social networking communities

Many UGC and social networking services include user obligations and rules within their terms and conditions – though these can read more like legal documents than useful advice for audiences. Some also provide more useful guidance: YouTube calls its rules *YouTube Community Guidelines;*[24] social networking site Habbo simplifies its rules in *The Habbo Way*[25], and gaming site RuneScape has *15 Rules of Conduct*[26], one of which details the types of language which are deemed to be offensive, including swear words (other rules deal with cheating and advertising).

22 http://sp.uk.ask.com/en/docs/about/site_policies.shtml.
23 http://uk.docs.yahoo.com/parents_guide/pledgesample.html.
24 http://uk.youtube.com/t/community_guidelines
25 http://www.habbo.co.uk/help/habbo_way.html
26 http://www.runescape.com/

Common elements in mainstream services like these, which are popular among children, focus on acceptable or prohibited content, including that which is seen as:

- bigoted, hateful, or racially offensive;
- abusive, defamatory, harassing, threatening or that could be deemed as stalking;
- pornography, sexually explicit;
- violent;
- promoting dangerous or illegal activities; or.
- subject to another party's copyright.

Of course, more specialist online communities also exist with quite different site characteristics - such as those focusing on pornography (YouPorn.com, PornoTube.com), or violent content (Extremevideos.org; Almostkillled.com) - whose content which clearly creates a risk of harm for children, or illegal copyright content (P2P sites like thepiratebay.org; and the recently closed Demonoid.com). However, this analysis focuses on mainstream services popular among children; such specialist communities are relatively easy to control through standard filtering software.

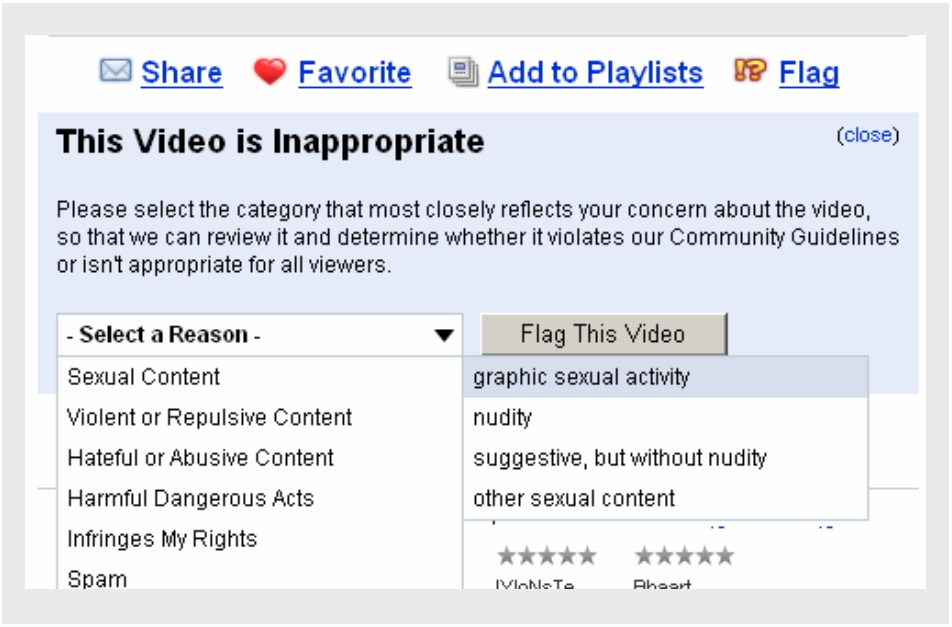
Mainstream websites universally assert their right to delete any content that violates their rules or conditions and state that the ultimate decision on what constitutes a breach will remain with the site operator.

The consequences of violating the terms are made clear – for example YouTube says that "violation of Terms of Use may result in a warning notification or may result in termination of your account and deletion of all your videos"; gaming site MiniClip warns that users "may be banned or accounts suspended or terminated";[27] and Piczo gives five examples of what action might be taken, from being issued with a warning to further legal action being taken.[28]

However, these sites do not give detailed guidance about the operation of the review processes. YouTube asserts that it reviews videos that have been flagged as inappropriate within 48 hours to determine whether they violate its terms of use. It also states that flagged videos are not automatically taken down by the system as human review is always involved.[29]

27 http://www.miniclip.com/games/en/terms-and-conditions.php
28 http://pic3.piczo.com/public/piczo2/piczoAcceptableUse.jsp
29 http://uk.youtube.com/t/community_guidelines

Figure 13: YouTube Flagging Options



Under UK and EU legislation, these types of UGC hosting service cannot be obliged to monitor the content they host (see Section 2.3). Some sites also assert in their terms of use that they are under no obligation to monitor their sites for inappropriate material. For example, MySpace declares in its terms that it "assumes no responsibility for monitoring the MySpace services for inappropriate content or conduct. If at any time Myspace.com chooses, in its sole discretion, to monitor the MySpace services, MySpace.com nonetheless assumes no responsibility for the content, no obligation to modify or remove any inappropriate content and no responsibility of the conduct of the user submitting any such content. [30]"

Online games sites operate in a broadly similar way, with defined rules of conduct and consequences regarding inappropriate behaviour, but also distance themselves from any obligation to remove material. For example, RuneScape and King.Com encourage users to flag inappropriate behaviour via their 'report abuse' buttons, but no time-scale is given as to when the complaint will be looked into or dealt with. RuneScape states that while it reserves the right to monitor and take action upon inappropriate use of the website (including the posting of inappropriate, offensive or otherwise objectionable material via the chat facility or otherwise), it cannot guarantee that it "will remove / modify any particular content." Similarly, MiniClip states that users' "inappropriate language and/or inappropriate behaviour is not allowed on MiniClip Limited websites" but states that "MiniClip limited is not responsible for user content, postings, chat, and/or communications. Users are responsible for their own actions." And King.Com states that it "does not actively monitor material which is contributed by members on the King.com service, and we make no undertaking to do so"

In mid-October 2007 Facebook committed to a process and timetable for dealing with complaints about nudity, pornography and unwelcome approaches, following an investigation by the New York attorney-general Andrew Cuomo. Under the new procedures, complaints regarding pornography and harassment are to be given priority among the tens of thousands of complaints received by the site every day. Facebook will have to respond to

30 http://www.myspace.com/index.cfm?fuseaction=misc.terms

such complaints within 24 hours and reply to the complainant reporting what steps it has taken within 72 hours. A third-party examiner is to report on its compliance for two years.[31]

However, of all the social networking, user-generated content and gaming sites we have looked at, this is the first example of a commitment to a target for complaint handling.

Other safety guidelines
In addition to content standards, the websites may also make other efforts to ensure that nobody is subjected to inappropriate content. These include age restrictions and safety guidelines.

Age restrictions/suggested ages
A number of sites give strict guidelines on the age users must be to use their services, while others just give general advice on suitability for various age groups.

Bebo, for example, states that users must be 13+[32]; MySpace states that users must be 14+[33] and photo-sharing site Slide states that users need to be at least 13 years old, adding that if they are under 18 years old they must get permission from their parent or legal guardian to use the service'[34].

Fantasy online gaming site RuneScape, on the other hand, recommends the game for players aged 13+ due to 'conflict and combat' and adds the guidance "if you wouldn't want your kids to watch 'Lord of the Rings', you probably wouldn't want them to play RuneScape".

Club Penguin states that it is designed for 6-14 year olds and is open to children of all ages, but unlike other social networking sites it strongly discourages the posting of any personal information including photos.

Safety guidelines
A number of sites including MySpace[35], YouTube[36] and Piczo[37] have introduced safety tips, which are usually located on the site's home page.

These safety guidelines contain general warnings that users should never post personal information such as "anything that could help a stranger find out who they are or where they live" and often also include links to online safety websites, such as Web Wise and Netsmartz, which give further information and guidance.

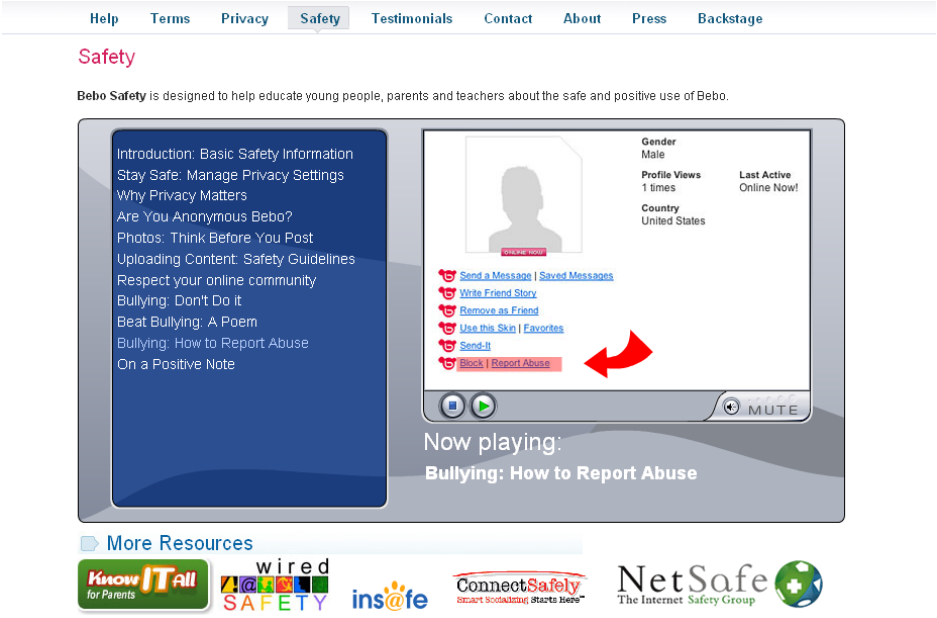
The tips also tend to contain advice that users shouldn't post items that may embarrass them later, and often stress the importance of reporting abuse, although they do not necessarily explain how to do this. For example, MySpace's tips just state that the user should: "talk with a trusted adult, or report it to MySpace or the authorities".

Bebo takes this one step further with a safety video, which simplifies the basic terms and conditions, shows how to stay safe on the internet and runs through how to report abuse and unacceptable content.

---

31 Details on NY Attorney General website at:
http://www.oag.state.ny.us/press/2007/oct/oct16a_07.html
32 http://www.bebo.com/TermsOfUse.jsp
33 http://www.myspace.com/index.cfm?fuseaction=misc.terms
34 http://www.slide.com/static/terms
35 http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safetytips
36 http://uk.youtube.com/t/safety
37 http://pic3.piczo.com/public/piczo2/safety/safety.jsp

Figure 14: Screen print from Bebo online safety video



2.8.2 Peer-to-peer networks

Content standards and take-down procedures

Peer-to-peer (P2P) networks differ from SNS, UGC and online gaming sites in the way they approach content controls and site rules. Several of the sites we looked at (including The Pirate Bay, Mininova and Limewire) set out their approaches to controlling content within their safety policies, copyright policies and FAQs. Some sites, including BitTorrent[38] and Soulseek,[39] do provide clear terms and conditions.

Some P2P site operators focus their efforts on controlling copyright content – though others exist largely in order to facilitate the unlicensed sharing of copyright material. Limewire has tried to work with copyright holders and the recording industry to develop a tool to filter out copyrighted material. The filter is currently being beta tested.[40] Mininova has a policy of removing its torrent files of copyrighted material if requested to do so by copyright holders. In contrast, The Pirate Bay aggressively asserts, when threatened, the legality of its service, and has a policy of publicly posting and lampooning any legal threats it receives on its website.[41]

Copyright infringement is potentially a serious concern for parents. Copyright holders have not shrunk from suing children or even parents of children where they believe illegal file sharing has taken place.[42]

In terms of control of content itself, approaches vary. The Pirate Bay and Limewire allow adult content to be shared, although the user must register to access adult content on The Pirate Bay; this is free and requires only an email address. Limewire provides a 'Family Filter' which can be switched on to 'ignore adult content' though it is not watertight.[43] Some

38 http://www.bittorrent.com/termsofuse.
39 http://www.slsknet.org/tos.html.
40 http://register.limewire.com/filter/
41 http://thepiratebay.org/legal.
42 http://www.networkworld.com/news/2006/101706-recording-industry-sues-another-8000.html.
43 http://www.limewire.com/support/ftc4.php#help3.

sites such as Mininova ban sexual or violent content altogether, though it is not clear how effectively this is enforced.

Age restrictions/suggested ages
None of the sites we looked at specified an age limit for users. Some suggest that parents should supervise children while they use the site, and Limewire is a good example of this.[44] Several sites (including The Pirate Bay) warned that users could come across unwelcome content, but that this was a hazard of using the site.[45]

2.9 Online advertising controls

As discussed in Annex 1, online advertising is a fast-growing segment of the advertising market. While it generally offers greater transparency and tracking capabilities than other media, website content is the least transparent segment of online advertising. This is partly due to problems with the definition of content, and also because websites often contain user-generated content that is difficult to define in advance. This may result in a situation where inappropriate adverts are displayed to audiences not intended to see them by the advertisers (for example, alcohol advertisements may appear on websites used by children and teenagers). Another concern is the appearance of adverts next to unsuitable content – for example, when banner advertisements for Apple iTunes appeared on illegal music download services.

A number of mechanisms are being put in place by the advertising industry to minimise such occurrences, mainly concerned with eliminating possible damage to the value of the advertised brands. Examples of these efforts include the code of practice implemented by the Internet Advertising Sales House (IASH), content categorisation by networks and affiliate networks and Google's *Adsense* programme.

IASH code
One of the purposes of IASH is to encourage good practice among online advertising sales houses. IASH has a code of conduct to which all its members are obliged to sign up. The purpose of the code is to ensure that all parties involved in the buying and selling of advertising space are aware of the types of content site that can and cannot be used for placing an advert.[46] The categories that IASH members are forbidden to use are:

- hate content, obscenity and indecency;
- bombs, guns, ammunition;
- invalid clicks (non-human clicks); and
- spyware.

Other inventory categories are permitted to IASH members only if they have been agreed and documented in advance by the client. These are:

- adult;
- peer-to-peer;

44 Ibid.
45 http://thepiratebay.org/about.
46 http://www.iash.org.uk/

- file sharing;
- incentivised clicks;
- adware;
- moderated forums; and
- anywhere that the code requesting the ad isn't owned by the publisher.

IASH is conducting an audit of all its members to try to ensure that they are complying with the code. However, in an interview with *New Media Age* in September 2006, the Chief Executive of IASH admitted that it was not possible to verify this down to the last site.[47]

A similar problem applies to websites featuring user-generated content – for example where users can upload their own audiovisual content, or which feature discussion fora. Advertisements placed on these types of sites can end up next to inappropriate content – next to material with which an advertiser would not want to be associated. For example, in August 2007 *The Guardian* reported that Virgin Media, Halifax, the Prudential, the AA, Vodafone and First Direct had all withdrawn their advertising from Facebook because their ads had been randomly placed on pages promoting the British National Party.[48]

Affiliate networks

Affiliate networks are similar to advertising networks, but operate on a 'pull' system, whereby a publishers signs up to be an affiliate and then applies to advertisers for the opportunity to promote and link to the advertiser's selected web page. However, the pricing model for affiliate networks is generally different - advertisers pay on a cost per action basis (see below for further details of pricing models).

Affiliate networks also seek to maintain restrictions on the types of publishers that may sign up to them. For example, when a publisher applies to become an affiliate on the Commission Junction http://www.cj.com/ network, it must agree not to engage in various activities including:

- misleading others;
- operating or linking to a website that contains or promotes libellous, defamatory, obscene, pornographic, abusive, violent, bigoted, hate-oriented, or illegal content;
- operating or linking to a website that offers any illegal goods or services; or
- engaging in spamming, indiscriminate advertising or unsolicited commercial email.

Google

In addition to its search advertising programme, where selected adverts are displayed alongside search results, Google also operates a system whereby publishers can feature Google links to another website, and thereby generate revenue. This is known as its '*Adsense*' programme.

47 http://www.nma.co.uk/Articles/29252/IASH+admits+auditing+isn't+rigorous+enough.html
48 http://www.guardian.co.uk/uk_news/story/0,,2141300,00.html

Publishers signing up to *Adsense* must agree that their sites do not include any of a range of content types including:

- violent or racially intolerant content;
- pornography, adult or mature content;
- gambling or casino-related content;
- sales or promotion of beer, hard alcohol, tobacco or prescription drugs; or
- any other content that is illegal, promotes illegal activity or infringes on the legal rights of others.[49]

2.10 Mobile content controls

Mobile phone ownership is nearly universal among older children and teenagers, and high among younger children. In addition, mobile phones are a much more personal medium, and parents may have limited ability to supervise their children's access to online content. Although relatively low at present, mobile access to internet content by children and teenagers is growing: the mobile internet experience is improving with rapid development in phone technology, usability, service innovation, and falling connection costs.

Children can access potentially harmful content on operators' portals as well on the wider internet.[50] Mobile operators have a significant role to play in offering parental controls and in ensuring that content inappropriate for children is protected by an effective age verification process.

Code of practice
The UK mobile operators have long recognised the child protection issues associated with mobile access. A joint industry code of practice was adopted by the six UK mobile operators (Vodafone, Orange, T-Mobile, 02, 3 and Virgin) in January 2004. The code details the actions that operators will take to control access to Illegal and potentially harmful content by children in the UK.

49 https://www.google.com/adsense/support/bin/answer.py?answer=48182&sourceid=aso&subid=ww-ww-et-asui&medium=link

50 Another area of concern, which falls outside of the scope of this submission, is content that entirely bypasses mobile operator networks and is exchanged via phone connectivity technologies such as Bluetooth.

Figure 15

Mobile operators' code of practice - summary of relevant provisions

- Mobile operators committed to apply a framework for classifying commercial content offered as part of their own service that is unsuitable for customers under the age of 18
- Commercial content providers will be required to classify as '18' all content unsuitable for customers under the age of 18. By default, all commercial content not classified as '18' will be unrestricted. Each mobile operator will place commercial content classified as '18' behind access controls and only make it available to those customers that it has satisfied itself, through a process of age verification, are 18 or over.
- The mobile operator will also place behind access controls all commercial content chat rooms, unless they are moderated chat rooms.
- Mobile operators have no control over internet content but will offer parents and carers the opportunity to have the mobile operator's internet access service filtered. The filter will be available at a level to filter out content approximately equivalent to commercial content with a classification of 18.
- Mobile operators will work with law enforcement agencies to deal with the reporting of content that may break criminal law. Where a mobile operator is hosting content, including web or messaging content, it will put in place notify and take-down provisions.
- Mobile operators will provide advice to customers - including children, parents and carers - on the nature and use of new mobile devices and services and support other relevant media literacy activities designed to improve consumers' knowledge.

The code requires the operators to support law enforcement agencies in tackling illegal content. All UK mobile operators are members of the Internet Watch Foundation, and mobile users with WAP-enabled phones can submit reports of illegal content to the IWF hotline via WAP.

The operators are responsible for classifying commercial content offered via their portals according to a classification framework developed by the IMCB[51], and to make 18+ content available only to users who have presented proof of age.

The classification framework was developed to be consistent, as far as possible, with standards for other media, produced by the British Board of Film Classification (BBFC) for film and by the Interactive Software Federation of Europe (ISFE)/ Pan-European Game Information (PEGI) for mobile games.

The framework applies only to commercial content offered via operator portals and does not cover content accessed on the wider internet. Content types covered by the IMCB classifications are:

- still pictures ;
- video and audiovisual material; and
- mobile games, including java-based games.

51 http://www.imcb.org.uk/classificationframe/

The framework excludes text, audio and voice-only services, gambling services (which are already age-restricted by UK legislation), chat rooms, location-based services (which are subject to a separate code of practice), and content generated by subscribers.

Figure 16

The IMCB classification framework - content unsuitable for those under 18

Themes
No theme is specifically prohibited though these may be subject to other legal requirements. Content must not actively promote or encourage activities that are legally restricted for those under 18 such as drinking alcohol or gambling.

Language
Frequent and repetitive use of the strongest foul language.

Sex
Actual or realistic depictions of sexual activity, for example,

- Real or simulated sexual intercourse.
- Depiction of sexual activity involving devices such as sex toys.
- Sexual activity with visible pubic areas and/or genitals or including threats of sexual violence such as rape.

Note, however, that material which genuinely seeks to inform and educate such as in matters of sexuality, safe sex and health and where explicit images are the minimum necessary to illustrate and educate in a responsible manner may be permissible.

Nudity
Nudity where depicting pubic area and/or genitals (unless it is material which genuinely seeks to inform and educate such as in matters of sexuality, safe sex and health and where explicit images are kept to the minimum necessary to illustrate and educate in a responsible manner).

Violence
Graphic violence which in particular dwells on the infliction of pain, injuries or scenes of sexual violence. In respect of mobile games in particular:

- Gross violence towards realistic humans or animals such as scenes of dismemberment, torture, massive blood and gore, sadism and other types of excessive violence.
- Graphic, detailed and sustained violence towards realistic humans and animals or violence towards vulnerable or defenceless humans.

Drugs
Depictions which promote or encourage illegal drug taking or which provide instructive details as to illegal drug taking.

Horror
Any depiction of sustained or detailed inflictions of pain or injury including anything which involves sadism, cruelty or induces an unacceptable sense of fear or anxiety.

Imitable techniques
Dangerous combat techniques such as ear-claps, head-butts and blows to the neck or any emphasis on the use of easily accessible lethal weapons, for example knives. Detailed descriptions of techniques that could be used in a criminal offence.

UK mobile operators also commit to offering network-layer filters for wider internet content accessible on mobile phones; all mobile operators in the UK currently offer such filtering solutions.

The UK operators and their parent companies have signed up to the new European Framework for Safer Mobile Use by Younger Teenagers and Children, adopted in February 2007[52]. This framework commits EU operators to implement measures that are already in place in the UK, and it is not expected to affect the self-regulatory arrangements in the UK market.

There is little evidence available on the potential for accessing harmful content via mobiles, and the effectiveness of current measures:

- It is unclear to what extent current practices are effective in protecting children. Our survey evidence suggests that fewer than 1% of children have encountered potentially harmful online content on their mobiles, although almost 1 in 4 parents expressed concern over this possibility[53]

- Concerns also have been raised as to whether the binary split (under and over 18) adequately reflects the need of children and teenagers. [54]

- There are indications of a lack of uniformity in applying controls. For example, in some cases contract customers are automatically considered to be over 18 as they will have confirmed their age upon registration. This means that if phones are passed on to children by parents, controls will not be in place, and parents will have to ask the operator to apply a filter.

The UK code of practice for the self-regulation of new forms of content on mobiles was published on 19 January 2004. Since that time the mobile market has developed and the range of content and services available has grown as a consequence. Ofcom believes it is timely to review the code to ensure it is still applicable and effective in providing a tool to protect children from access to inappropriate content on mobile phones. Ofcom, in partnership with the Home Office and the Children's Charities Coalition on Internet Safety, has begun an audit which will result in the publication of a review with recommendations in 2008.

2.11 Controlling illegal online content

Several types of activity with online content are illegal in the UK
There is a distinction between content that is illegal, and content that, although legal, is potentially harmful to adults and/or children. In the UK, activities relating to the possession and distribution of online content which are illegal include:

- Taking, permitting to be taken, making (including downloading or printing for private use), possessing, showing, distributing or advertising indecent images of children in the UK (Protection of Children Act 1978, The Criminal Justice Act 1988, Sexual Offences Act 2003).

- Publishing, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it

52 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3153
53 Data from Ofcom research October 2007. Full details, including methodology, in Annex 5
54 e.g. by ICRA
http://ec.europa.eu/information_society/activities/sip/docs/public_consultation_mobile/results/icra_a337318.pdf

(or to have an obscene article for publication for gain) (Obscene Publications Act 1959 and 1964).

- Publishing content which is defamatory - that is, tending to lower a person in the estimation of right-thinking members of society or cause him to be shunned or avoided; refer to a living individual or entity (Defamation Act 1996)

- Sending a message or other matter by means of a public electronic communications network that is grossly offensive or of an indecent, obscene or menacing character or causing such to be sent (Communications Act 2003).

- For the purpose of causing annoyance, inconvenience or needless anxiety to another, sending by means of a public electronic communications network a message that person knows to be false, causing it to be sent or persistently making use of such a network (Communications Act 2003).

- Using or publishing insulting or abusive words (or behaviour) with intent to stir up racial hatred or likely to do so in the circumstances (and to possess material with a view to distribution and an intent to stir up racial hatred) (Public Order Act 1986, Public Order Act 1986, Crime and Disorder Act 1998, Criminal Justice Act 2003 and Racial and Religious Hatred Act 2006)

- Publication of statements that are likely to be understood as direct or indirect encouraging of terrorism and dissemination of terrorist publications. (Terrorism Act 2006)

A co-regulatory approach to enforcing the regulation of illegal online content
Monitoring and removal of illegal content in the UK is carried out via a partnership between police, government and the industry, involving a number of organisations, listed below.

The Internet Watch Foundation (IWF)
The IWF is a regulatory body set up in 1996 following an agreement between government, the police and the UK online industry. Its key objective is to minimise the availability of potentially illegal internet content, specifically:

- child sexual abuse images hosted anywhere in the world;

- criminally obscene content hosted in the UK; and

- incitement to racial hatred content hosted in the UK.

The IWF works in partnership with UK government departments such as the Home Office, the Ministry of Justice and the Department for Business, Enterprise and Regulatory Reform to influence initiatives and develop programmes to combat online abuse.

The IWF is funded by the EU and the wider online industry. This includes internet service providers (ISPs), mobile operators and manufacturers, content service providers, telecommunications and filtering companies, search providers and the financial sector as well as blue-chip and other organisations.

Figure 17

The IWF - key activities

- Acts as a hotline for reporting illegal and obscene content on the internet, and assists law enforcement agencies in the UK and abroad in dealing with illegal content.
- Issues take-down notices to hosting service providers relating to reported content which is deemed by the IWF to be illegal, and is hosted in the UK. If the content is illegal but hosted outside the UK, the IWF notifies the relevant authorities in the country of jurisdiction.
- Maintains a regularly updated database of all IP addresses hosting illegal content in the UK and abroad. The database is provided to UK ISPs who can voluntarily choose to block their users' access to the listed addresses.
- Supplies ISPs with details of online user groups dedicated to disseminating illegal and offensive material, and recommends that they be blocked by ISPs.
- Provides information for internet users on how to protect themselves using filtering services and other tools

As described in Figure 17 above, the IWF is the main body dealing with the illegal online content in the UK. It serves as the UK's only national hotline, and is the UK member of the EU-wide hotline network, INHOPE. It enforces the notice and take-down regime for illegal content, and co-operates with law enforcement authorities in the UK and abroad.

The IWF also invests significant effort in promoting information about safe internet use by developing and disseminating materials for teachers, parents and children and carrying out information campaigns.

It enables network-layer filtering of illegal content by the UK ISPs, based on its database of websites containing illegal material. The database is regularly updated and contains between 800 and 1200 live child abuse URLs at any one time. It applies to websites only and does not cover other means of distributing illegal images such as peer-to-peer networks.

According to the Internet Services Providers Association (ISPA), all major ISPs, and most smaller ones, use the database to block access to the sites listed in the database. This means that the vast majority of consumer internet connections are protected against accessing illegal content listed in the database.

The internet Service Providers' Association (ISPA)

The Internet Service Providers' Association contributes to the policing of illegal content. It requires its members to comply with take-down notices issued by the IWF and requires ISPs to provide relevant user details to the police. ISPA co-operates with the IWF in its efforts to remove illegal material from internet websites and newsgroups. Members are therefore required to adhere to the following procedures in dealing with the IWF:

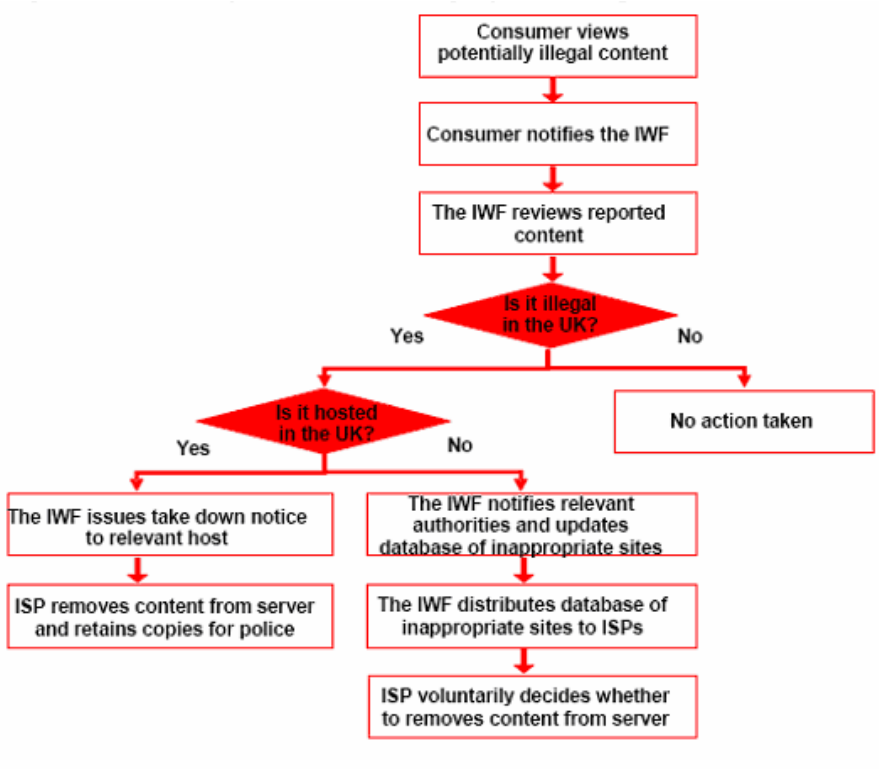
- provide ISPA with a point of contact to receive notices from the IWF;
- when notified by the IWF, remove internet sites and/or Usenet news groups they host containing material which the IWF considers to be illegal child abuse images;
- when requested by the IWF or a legitimate law enforcement authority, and wherever technically able to do so, retain copies of removed material for a reasonable period of time; and

- take careful consideration of all other IWF notices and recommendations.

ISPA's code of practice encourages participating ISPs to join the IWF. Non-compliance with the code of practice results in sanctions, which may include suspension of membership.

The relationship between the IWF and the ISPs is illustrated in the diagram below.

Figure 18: The IWF process for handling reports of illegal content



The Home Office Internet Task Force for Child Protection

The task force, established in 2001, aims to improve safety of internet use for children in the UK, and to help protect children across the world from abuse fuelled by criminal misuse of new technologies.

Chaired by the Home Office Minister Vernon Coaker, it is a partnership between the Government, the police, internet industry representatives and child welfare organisations. Its key areas of activity are improvements in chat room supervision and provision of safety information to children online.

Cyberbullying task force

The task force was established by the Department for Children, Schools and Families in spring 2007 to tackle all aspects of cyberbullying. It includes a broad range of participants, including from the communications industry (internet service providers; mobile phone companies and social networking services), teachers' associations, children's charities, and law enforcement agencies. The task force proposes innovative and practical solutions to cyberbullying, including a planned digital information campaign for children and young people and guidance for school staff.

Metropolitan Police Specialised Crime Directorate

The Directorate's Child Abuse Investigation Command investigates child abuse and deals with paedophile issues across London, working closely with other child protection agencies. The Command's Hi Tech Crime Unit provides technical computer support and is able to arrest and prosecute offenders who target children through the internet.

The Child Exploitation and Online Protection Centre (CEOP)

CEOP was launched in the UK in 2006 and aims to apply a holistic approach to protecting children online, combining police powers with the dedicated expertise of business sectors, government, specialist charities and other organisations. It manages the flow of information across the UK and with international agencies, and works to locate perpetrators and track registered offenders who have failed to comply with their notification requirements.

The Centre also identifies victims of online abuse and liaises with the industry to help minimise the use of technology for the sexual abuse of children. Its activities include campaigns to raise awareness of child abuse issues among parents, children, young people and the stakeholder community.

CEOP works with police forces to minimise the volume, risk and impact of abuse and to provide an effective law enforcement response. It seeks to reduce the profits to organised crime arising from the distribution of illegal images, and provides support for local forces in areas such as computer forensics and covert investigations.

Other organisations

A number of other organisations are also actively involved in tackling online crime, and in particular, child abuse, including:

- **The British Educational Communications & Technology Agency (BECTA)** which supports the work of the Internet Task Force in the area of education.

- **The Children's Charities Coalition for Internet Safety (CHRIS**) which brings together leading UK charities working to support the fight against child abuse and child protection online (NCH, Barnardos, Childline, The Children's Society, National Children's Bureau, NCVCCO, NSPCC, ECPAT and StopIt Now!).

- **End Child Prostitution, Child Pornography and the Trafficking of Children for Sexual Purposes** (ECPAT) is a children's rights organisation campaigning against the commercial sexual exploitation of children in the UK and the international aspects of trafficking.

- **The National Council of Voluntary Child Care Organisations** (NCVCCO) is an umbrella body for the voluntary and community sector in England.

- **StopIt Now!** is a campaign that aims to stop child sexual abuse by encouraging abusers and potential abusers to seek help and by giving adults the information they need to protect children effectively. The campaign is supported by a range of organisations, including children's charities and government agencies.

Reduction in share of illegal images hosted in the UK

As a result of the activities of the IWF and other relevant organisations, there has been a great reduction in illegal content hosted in the UK. According to the latest available statistics, the share of illegal content hosted in the UK reduced from 18% in 1997 to less than 1% by the end of 2006.

Despite the success of the IWF in reducing UK-based illegal content, there are signs of an increase in the amount of illegal content around the world. Although not hosted in the UK, this content can be easily accessed by UK internet users. According to INHOPE data, the volume of reports to European hotlines about illegal and harmful content continues to increase by about 13% a year. Half of all reports in the last quarter of 2006 were about suspected child abuse images.

The IWF reported a significant increase in URLs containing child abuse images, from 6,128 in 2005 to 10,656 in 2006. It also reported a slight increase in the total number of domains hosting such images, from 2,966 to 3,077 over the year. Over 85% of all of these domains were traced to the US and Russia.

International co-operation in combating illegal content

There is extensive international co-operation on tackling child abuse images; unlike many other types of content, child abuse material is illegal nearly everywhere in the world. Key intergovernmental organisations, including the UN and the Council of Europe, have supported efforts to facilitate co-operation between countries on the issues. The international legal framework addressing online images of child abuse has evolved at a number of levels:

- The International Labour Organization's Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour, Convention 182 (1999) has 132 State Parties. The Convention aims to eliminate the worst forms of child labour, which include "the use, procuring, or offering of a child for . . . the production of pornography or for pornographic performances." For the purpose of this convention, a child is anyone under the age of 18.

- The 2000 UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography mandates its signatory nations to prohibit the sale of children, child prostitution and child pornography, including via the internet, within their nation's law,. It also provides a framework for increased international co-operation in prosecuting perpetrators in these areas. The Protocol been ratified and is in force in 12 nations.

- The 2001 European Convention of Cybercrime mandates its signatories to prohibit the production, distribution and buying of child pornography over the internet. It was the first international treaty to criminalise offending behaviour directed against computer systems, networks or data in addition to content-related crimes such as child pornography. The Convention creates a legislative framework for investigating and prosecuting violations of law with respect to child abuse material, and mandates co-operation between national agencies in combating child pornography. As of 31 October 2007, the Convention had been signed by 43 countries and ratified by 21 countries. The UK signed the Convention in 2001 but has not yet ratified it.

Several international initiatives have been set up to collaborate in tackling the issue of child abuse images. The EU's *Safer Internet Programme* (SIP) aims to promote safer use of the internet and new online technologies, particularly for children, and to fight against illegal

content and content unwanted by the end-user, as part of a coherent approach by the European Union. The programme has four activities: hotlines; awareness-raising activities; tackling unwanted and harmful content; and promoting a safer environment. The programme's first phase ran from 1999 to 2004 and financed over 80 projects with a €38.3m budget. The second phase, *Safer Internet Plus,* runs from 2005 to 2008 and has a budget of €45m.

The Association of Internet Hotline Providers in Europe (INHOPE) provides a collaborative forum for hotlines from all over the world.

Figure 19

INHOPE - aims and objectives

The mission of the INHOPE Association is to support and enhance the performance of internet hotlines around the world, ensuring swift action is taken in responding to reports of illegal content to make the internet a safer place. To achieve this mission, INHOPE has five specific objectives:

- To establish policies and best practice standards for hotlines and encourage exchange of expertise among members through fostering good working relationships and trust.
- To ensure rapid and effective response to illegal content reports around the world by developing consistent, effective and secure mechanisms for exchanging reports between hotlines internationally and ensuring a coordinated approach is taken.
- To expand the network of INHOPE members around the world by identifying and supporting new hotlines to become members by providing consultation and training to meet best practice standards.
- To promote a better understanding of the work of hotlines to policymakers at an international level, including government, law enforcement and other related bodies, with the aim of achieving better co-operation internationally.
- To raise awareness of INHOPE and member hotlines with key stakeholders as well as the general public as a "one stop shop" for global reports of illegal content from around the world.

Another body operating at the European level is INSAFE, a network of national nodes that coordinate internet safety awareness. CEOP is the UK node on this network.

In addition to EU-wide measures, the *Virtual Global Taskforce* (VGT) was set up in 2003 to provide a forum for global collaboration in tackling child abuse images. The VGT is made up of law enforcement agencies from around the world working together to fight child abuse online.

Figure 20

The Virtual Global Taskforce – aims and objectives

The aim of the VGT is to build an effective, international partnership of law enforcement agencies that helps to protect children from online child abuse.

The objectives of the VGT are:
- to make the internet a safer place;
- to identify, locate and help children at risk; and
- to hold perpetrators appropriately to account.

The VGT is made up of the Australian High Tech Crime Centre, the Child Exploitation and Online Protection Centre in the UK, the Royal Canadian Mounted Police, the US Department of Homeland Security and Interpol. Jim Gamble, the Chief Executive of the Child Exploitation and Online Protection Centre is the Chair of the VGT.

The VGT has a website (www.virtualglobaltaskforce.com) providing information, advice and support to children. It offers a facility to report suspicious behaviour to law enforcement agencies in Australia, Canada, the United States and the UK. Another initiative launched by the VGT is '*Operation PIN*' – a website purporting to contain images of child abuse – which captures details of individuals seeking to download images from the site.

International collaboration in areas other than child abuse has proved problematic

Attempts to encourage international collaboration on other types of inappropriate content have had limited success, due to national differences in defining what is 'inappropriate'. The committee drafting the Cybercrime Convention discussed the possibility of including content-related offences other than child pornography (Article 9) within the Convention; for example, the online distribution of racist propaganda. However, the committee could not reach consensus on the inclusion of additional offences within the Convention. Instead, it recommended that additional protocols to the Convention should be developed under the title '*Broadening the scope of the convention to include new forms of offence*'.

The *Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems* aims to harmonise substantive criminal law in the fight against racism and xenophobia on the internet and to improve international co-operation in this area. Following five ratifications, it came into force on 1 March 2006. Importantly, however, the UK and the US are currently not signatories to the Additional Protocol.

Although the US signed the original convention which focused on child pornography, it has not signed the Additional Protocol on the grounds that this protocol restricts an individual's right to free speech. The First Amendment of the US Constitution guarantees an individual's right to free speech and is broader in scope than the equivalent Article 10 of the European Convention of Human Rights. The First Amendment states that 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances'.

Such differences in national opinion compromise the effectiveness of the treaty. Websites containing offensive content, in this instance racist or xenophobic content, can relocate their hosting to a country which is not a signatory to the treaty, thereby avoiding legal sanctions.

Section 3

Educational initiatives: raising awareness of safe internet use

3.1 The role of media education in formal education

The following section outlines the place of media education generally (and the specialist subject of media studies) and media literacy in formal education in the UK[55].

3.1.1 Curriculum

Although communications media feature as teaching and learning resources throughout much of the curricula at pre-GSCE stages, media education is primarily focused in the following areas:

- Languages - English, Welsh, Language and Literacy – including the study of print and audio-visual texts.
- Citizenship and PSHE/PSE/Personal Development and Understanding/People in Society - the significance of communications media in society, their influence, roles and responsibilities; developing skills in democratic participation.
- ICT – including a focus on the analysis and evaluation of information.

Generally, while there are opportunities within Key Stages 1 and 2 for links with the media to be made within wider learning areas (e.g. critical understanding), this is rarely explicit. Key Stages 3 and 4 mark the start of a greater emphasis on the study of media for their own sake. The new curriculum in Northern Ireland places greater emphasis on the media from the early stages.

The new Secondary Curriculum in England will be phased in from 2008. For the purposes of this section, the main points of interest are: the explicit inclusion at Key Stage 3 ICT of critical evaluation and e-safety, and the introduction of a cross-curriculum dimension in Technology and the Media. The Scottish curriculum is currently going through a national review entitled Curriculum for Excellence with the aim of developing a streamlined curriculum for 3-18-year-olds and implementing new approaches to assessment.

3.1.2 Qualifications

The Welsh Baccalaureate, rolled out from September 2007, includes aspects of the study of the media. In Scotland there is the opportunity to study Media Studies at Intermediate 1, 2, Higher and Advanced Higher levels. Elsewhere in the UK, Media and Film Studies is offered at GSCE and A Level, in addition to a variety of vocational courses.

Specialised Diplomas are new, employer-led qualifications which will enable 14 to19 year olds to pursue studies focused on a range of vocational subjects, including Information Technology, Creative and Media and Society, Health and Development. From 2008 there will be a national diploma in Creative Media – this is also being considered for inclusion in the Welsh Baccalaureate.

55 excluding the role of pre-primary Foundation stages.

3.1.3 E-safety

Although e-safety is not explicitly referred to within the National Curricula at present, (with the exception of Northern Ireland) there are a number of areas within the programmes of study that offer opportunities to discuss e-safety issues, and these are highlighted within Becta publications[56]. It is accepted best practice, although not a legal requirement, for schools to have a policy for pupils' acceptable use of the internet, including aspects of e-safety. Ofsted's schools' self-evaluation framework (SEF) has recently been updated to incorporate e-safety. The DCSF has recently responded to concerns about cyberbullying by launching new guidance[57] for schools to help tackle cyberbullying as part of its "*Safe to Learn*" initiative.

3.1.4 Summary

While the information above is intended to give a flavour of the curricular requirements in the nations, relatively little is known about what is actually happening in these areas in schools – there has been no substantial research about media education in schools. There is also debate about the adequacy of provision of professional support/training for teachers in this area.

3.2 Education-based initiatives

In this section we list the various initiatives under way:

- **Centre for Child Exploitation and Online Protection** - Over 1.1 million children in schools across the UK have attended the Child Exploitation and Online Protection (CEOP) Centre's interactive ThinkUKnow sessions. The centre has recently launched a new initiative "Purely for Parents" to bring parents and guardians more up to speed with the way in which the internet is integral to children's lives and to help them understand ways of making the online experience safer for children of all ages. The programme will be delivered both through specially designed parents' evenings at local schools and through an online facility at www.thinkuknow.co.uk/parents.

- **Childnet International** - has developed an e-safety resource, Know IT All, which is available free of charge to maintained primary and secondary schools in England. The series also contains a subsequent release, Know IT All for parents – which in its first six months has been distributed by schools to approximately one million parents. The resources have been translated into a range of languages including BSL, Arabic, Mandarin, Polish, Gujarati, Punjabi, Bengali and Urdu. www.childnet-int.org/

- Childnet also undertook a pilot programme to make teachers in their initial teacher training aware of e-safety issues relating to their pupils' use of the internet, both in the classroom and outside school. Based on research with academics and on this pilot, e-safety was recognised as a requirement for current teachers and the need for child e-safety training among trainee teachers was identified. As a result, Childnet is shortly to launch *Know IT All for Teachers* (KIA) – a resource aimed at helping teachers and trainee teachers understand and deal with e-safety issues within schools. The resource was developed by Childnet International and supported by the TDA, Microsoft and Becta. It provides a set of resources and outlines the various

56 Becta's site provides extensive guidance and support for the use of technologies in schools: www.becta.org.uk
57 The guidelines are available on the DCSF's Teachernet website at www.teachernet.gov.uk.

issues around e-safety. Childnet International has recently launched a website entitled Digizen which aims to support and showcase young people's positive social engagement and participation online.

- **Media Smart UK** - is a non profit-making media literacy programme for school children aged 6 to 11 years old, focusing on advertising. Media Smart develops and provides, free of charge and on request, educational materials to primary schools that teach children to think critically about advertising in the context of their daily lives. Their materials use real examples of advertising to teach core media literacy skills. Media Smart is funded by the advertising business in the UK and is supported by the UK and EU governments. It is the only programme in Europe that brings together the resources of the industry, expertise of leading academics and the advice of the government into one comprehensive national programme. http://www.mediasmart.org.uk/

- **Safer Internet Day** - is an opportunity to dedicate time in schools to reflect on some of the issues and to raise awareness of them. Each year there is a competition for schools. Almost 40 countries took part in Safer Internet Day 2007 (SID). The campaign is organised by European Schoolnet, coordinator of Insafe, the European safer internet network www.saferinternet.org.

- **Scottish Screen** - has launched a new investment strand for education initiatives. The fund has been set up to promote the development of moving image education and moving image media literacy, in both formal and informal educational contexts. Working with partners, Scottish Screen is currently piloting Moving Image Education in a variety of contexts, including early years, teacher education and professional development, and the Executive-funded programme in the Brechin cluster of schools. http://www.scottishscreen.com/

- **British Film Institute** - promotes greater understanding and appreciation of, and access to, the film and moving image culture in the UK and has a number of online resources available for use in schools: www.bfi.org.uk

- **Film Education** - is an industry-funded body providing free online material available to schools. It also runs an annual National Schools Film Week each October, which provides free screenings to over 150,000 primary and secondary pupils across the UK. http://www.filmeducation.org

- **The English and Media Centre** - publishes materials on moving image and print media and runs training courses. http://www.englishandmedia.co.uk/

- **BBC/C4** – initiated two new media literacy projects, the BBC News' 'School Report' and Channel 4's 'Breaking the News' which involved pupils in creating the news. The two projects have been held up as examples of the media industry working together creatively and strategically in meeting the challenge of engaging audiences with media literacy.

- http://news.bbc.co.uk/1/hi/school_report/default.stm

  http://www.channel4.com/learning/breakingthenews/index.html

- **Media Literacy Task Force** – the charter developed by the Task Force includes the statement that signatories support "…the principle that every UK citizen of any age should have opportunities, in both formal and informal education, to develop the skills and knowledge necessary to increase their enjoyment, understanding and

exploration of the media." A number of agencies in education, media and related industries have now pledged their support. www.medialiteracy.org.uk/taskforce/

- **Professional bodies** - there are a number of professional bodies supporting teachers and encouraging the sharing of best practice of media education including the Media Education Association, the Association for Media Education in Scotland, Media Education Wales and the Northern Ireland Media Education Association. www.mediaedassociation.org.uk

- **Local Safeguarding Children Boards (LSCB)** were established in 2006. The objective of LSCBs is to coordinate and to ensure the effectiveness of their member agencies in safeguarding and promoting the welfare of children. The core membership of LSCBs is set out in the Children Act 2004, and includes local authorities, health bodies, the police and others. To support the Boards' e-safety role, Becta has published "Safeguarding Children Online: a guide for Local Authorities and Local Safeguarding Children Boards.

3.3 Media literacy and Ofcom

Ofcom assumed its powers under the Communications Act 2003 on 29 December 2003. The promotion of media literacy is a new duty for Ofcom arising from Section 11 of the Act.

11 Duty to promote media literacy

(1) It shall be the duty of OFCOM to take such steps, and to enter into such arrangements, as appear to them calculated-

(a) to bring about, or to encourage others to bring about, a better public understanding of the nature and characteristics of material published by means of the electronic media;

(b) to bring about, or to encourage others to bring about, a better public awareness and understanding of the processes by which such material is selected, or made available, for publication by such means;

(c) to bring about, or to encourage others to bring about, the development of a better public awareness of the available systems by which access to material published by means of the electronic media is or can be regulated;

(d) to bring about, or to encourage others to bring about, the development of a better public awareness of the available systems by which persons to whom such material is made available may control what is received and of the uses to which such systems may be put; and

(e) to encourage the development and use of technologies and systems for regulating access to such material, and for facilitating control over what material is received, that are both effective and easy to use.

(2) In this section, references to the publication of anything by means of the electronic media are references to its being-

(a) broadcast so as to be available for reception by members of the public or of a section of the public; or

(b) distributed by means of an electronic communications network to members of the public or of a section of the public.

Purpose of Ofcom's work to promote media literacy

Ofcom's work to promote media literacy is intended:

- to give people the opportunity and motivation to develop competence and confidence to participate in communications technology/the digital society
- to inform and empower people to manage their own media activity (consumption and creation)

Having taken account of our duties in Section 11 Ofcom's role in respect of Media Literacy can be interpreted as:

To 'promote':

- access - Content management (i.e. Navigate and Manage)
- access - Control Systems – easy to use and effective technology and systems (i.e. Manage)
- understand - Critical awareness – (i.e. read and deconstruct)

Media Literacy is an umbrella term covering a set of skills, knowledge and understanding of the media and of communications technology - i.e. to be media savvy. It is an expert term, rather like PSB. While there are several definitions of media literacy, the **purposes** and **competences** of media literacy are more useful than the (very general) definition itself (*"The ability to access, understand and create communications in a variety of contexts*").

The following table outlines the key competences of media literacy:

Media literacy competences

Definition		Example Competences
Access	Use Navigate Manage	• Evaluate and use technology • Use an EPG and web browser • Access, store, retrieve content and services • Search effectively and safely • Customise applications • Use firewalls and filters
Understand	Read Deconstruct Evaluate	• Recognise editorial, advertising & sponsorship • Understand media contexts and motivations • Critique – i.e. have a view on quality and provenance of material • Make informed choices
Create	Produce Distribute Publish	• Use technology to communicate ideas, information and opinions • Contribute to the democratic process using electronic media • Post and transact online • Use media responsibly

Some findings from Ofcom's Media Literacy Audit (2006) about children's use of the internet at school

Ofcom's Media Literacy Audit[58] (2006) found that children aged 8-11 are significantly more likely to prefer to learn about digital technologies from school (48%) and from their parents (45%) than those aged 12-15. By contrast, the top choice for children aged 12-15 is to learn about digital technologies from friends - learning from school is the second most popular nomination from 12-15s (41%). By nation, children in England and Northern Ireland are significantly more likely to prefer to learn from school (at 46% and 47% respectively) than those in Wales and Scotland (at 37% each).

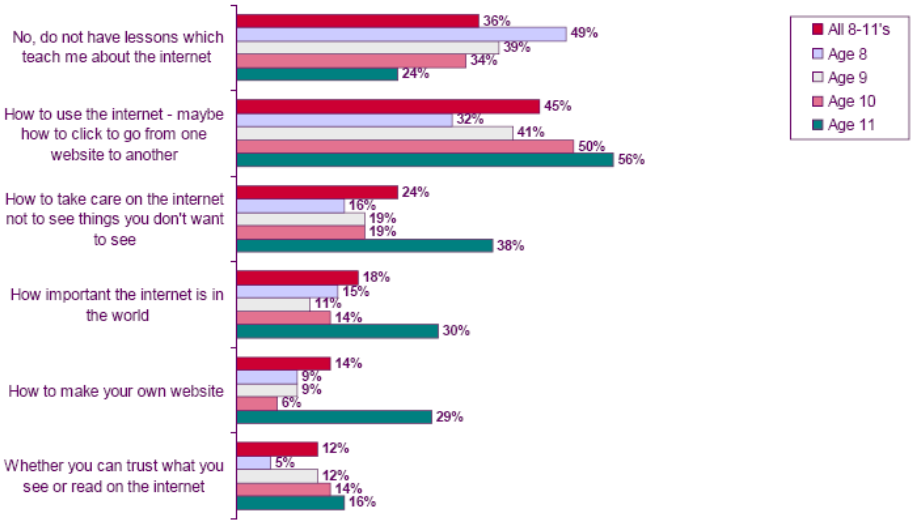
Children aged 8-11 were asked whether they had any lessons at school which taught them about the internet and also whether they had any lessons at school which taught them about television or films. Those who said they did have either type were prompted with possible types of things they may have learned about in these lessons and were asked to say which applied to them.

Around two-thirds (64%) of all children aged 8-11 said they had any lessons which taught them about the internet, and just one in ten in this age group (9%) said they had any lessons which taught them about television or films. Both types of lessons were more common among the oldest children (aged 11) in this age group, rising to 76% for lessons about the internet and 15% for lessons about television or film.

Figure 21 below, shows responses regarding lessons about the internet both overall for all 8-11 year olds and for each of the four ages within this overall age group.

58 http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/children/

Figure 21: Lessons for 8-11s about the internet at school[59]



As shown in Figure 21, while a majority of 8-11s have lessons about the internet at school, responses from 11 year olds differed significantly from those children aged 8-10, with each type of learning being significantly more common among 11 year olds, with the exception of 'whether you can trust what you see or read on the internet'.

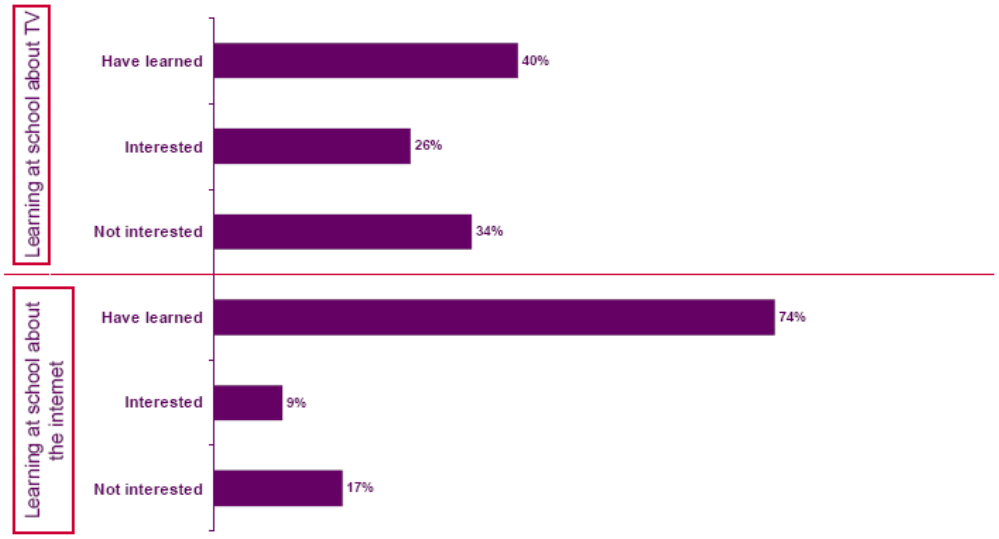
Responses also differed significantly by nation, with two-thirds (66%) of 8-11s in England and around three in five (58%) 8-11s in Scotland saying they had lessons about the internet, compared to around two in five of those in Wales (43%) and Northern Ireland (41%).

One in ten children (9%) aged 8-11 say they had any lessons at school about television or film. This is again rather more common in England (10%) and Scotland (7%) than in Wales (4%) and Northern Ireland (5%).

Children aged 12-15 were asked whether any of their lessons at school taught them about TV ('For example, how TV programmes are made and how they are paid for') and also whether any of their lessons at school taught them about the internet ('For example, how the internet works, how to make websites, or how to avoid websites you don't want to see'). All 12-15s were then asked whether they would be interested in learning more at school about these issues relating to TV and the internet. Figure 22 below summarises responses overall given by 12-15 year olds.

59 Base: All children aged 8-11 (772). Question QC60, prompted responses, multi-coded.

Figure 22: Lessons for 12-15s about TV and about the internet at school[60]

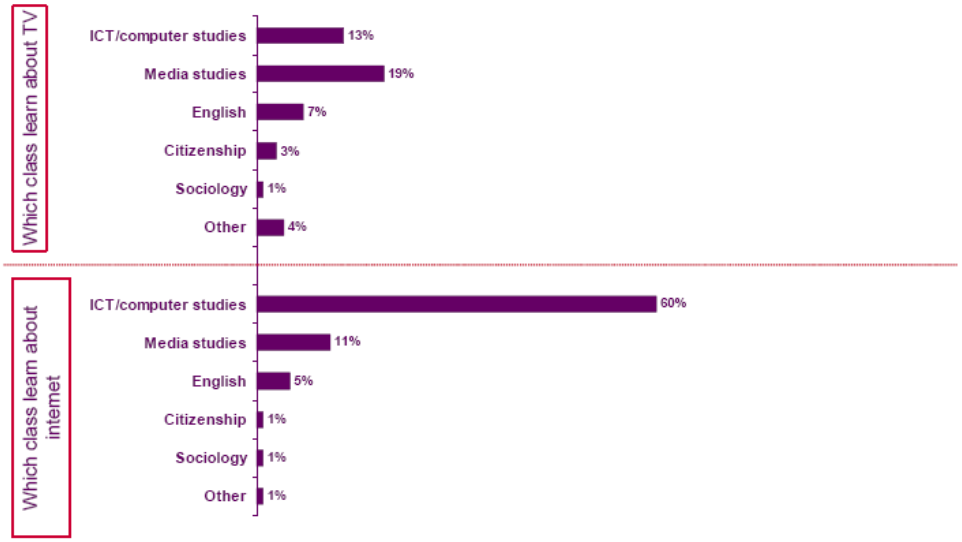


As indicated in Figure 22, 40% of 12-15s had learned about TV at school, and three-quarters in this age group (74%) had learned about the internet at school. A minority of children aged 12-15 had neither learned nor were interested in learning about TV (34%) or about the internet (17%). However, among those who didn't already have experience of this learning, a higher proportion were uninterested than interested.

Learning about the internet does not differ across England, Scotland and Northern Ireland (ranging between 73%-74%), but is significantly less common among those aged 12-15 living in Wales (63%).

Finally, we asked children in which classes they had learned about the internet and about TV.

Figure 23: In which class 12-15s learn about TV and the internet at school[61]



60 Base: All children aged 12-15 (764). Questions QC56-59, prompted responses, multi-coded.

61 Base: All children aged 12-15 (764). Question QC57, prompted responses, multi-coded.

As Figure 23 shows, 60% of 12-15s said that they learned about the internet from ICT or computer classes, although one in ten (11%) said they learned about it in media studies classes. One in five said they learned about television in media studies classes.

3.4 Media literacy and the BBC

The BBC is constitutionally established by a Royal Charter. The Charter sets out the public purposes of the BBC and guarantees its editorial independence. It prescribes the constitution of the BBC, the relationship between the Trust and the Executive Board, and the duties and functions of both bodies.

The current Charter was granted to the BBC on 19 September 2006 and came into force on 1 January 2007. It runs until the end of 2016. Under the new Charter, the BBC is governed by the BBC Trust, which sets the strategic direction of the BBC and has a clear duty to represent the interests of licence fee payers. The Trust sets public purpose remits[62], issues service licences[63] and holds the Executive Board to account for its performance in delivering BBC services.

The Agreement complements the Charter. It goes into more detail on many of the subjects mentioned in the Charter and also covers such things as the BBC's regulatory obligations and funding arrangements. The Agreement was made between the BBC and the Secretary of State for Culture Media and Sport, and approved after a debate in Parliament in July 2006.

The Charter

The Charter sets out the following:

The BBC's public nature and its objects

(1) The BBC exists to serve the public interest.

(2) The BBC's main object is the promotion of its Public Purposes.

…

The Public Purposes

The Public Purposes of the BBC are as follows—

(a) sustaining citizenship and civil society;

(b) promoting education and learning;

(c) stimulating creativity and cultural excellence;

---

[62] One of the BBC Trust's obligations is to set purpose remits for each Public Purpose. These define the Trust's priorities for the Executive Board and explain how it will judge the Executive's performance against them.

[63] The BBC Trust issues a licence for each of the BBC's UK public services. Service licences are used by the Trust to ensure that each BBC service creates public value by delivering the BBC's Public Purposes.

(d) representing the UK, its nations, regions and communities;

(e) bringing the UK to the world and the world to the UK;

(f) in promoting its other purposes, helping to deliver to the public the benefit of emerging communications technologies and services and, in addition, taking a leading role in the switchover to digital television[64].

Under the terms of the Charter and Agreement, the BBC's main activities should be the promotion of these public purposes through output consisting of information, education and entertainment.

The Agreement

The new BBC Agreement goes into detail about the duties of the BBC. It includes the following information about the Public Purpose "***Sustaining citizenship and civil society"***

(1) In developing (and reviewing) the purpose remit for sustaining citizenship and civil society, the Trust must, amongst other things, seek to ensure that the BBC gives information about, and increases understanding of, the world through accurate and impartial news, other information, and analysis of current events and ideas.

(2) In doing so, the Trust must have regard amongst other things to—

(a) the need to promote understanding of the UK political system (including Parliament and the devolved structures), including through dedicated coverage of Parliamentary matters, and the need for the purpose remit to require that the BBC transmits an impartial account day by day of the proceedings in both Houses of Parliament;

(b) the need to ***promote media literacy****; and*

(c) the importance of sustaining citizenship through the enrichment of the public realm.[65]

The words in bold in (b) are the only reference to the promotion of media literacy in the Charter or Agreement. Therefore in statutory terms, the promotion of media literacy is limited to the giving of information and increasing understanding of the world through accurate and impartial news, other information and analysis of current events and ideas.

The specific obligation is described as follows, in the draft remit:

Enable audiences to access, understand and interact with different types of media.

"The BBC should help people become 'media-literate' – giving them the confidence to make full use of information technologies. The BBC will help its audiences find what they are looking for from trustworthy sources, understand what it is about, have an opinion about it and where necessary, respond to it".

[64] From the BBC Charter: http://www.bbc.co.uk/bbctrust/assets/files/pdf/regulatory_framework/charter_agreement/royalcharterssealed_sept06.pdf

[65] From the BBC Agreement: http://www.bbc.co.uk/bbctrust/assets/files/pdf/regulatory_framework/charter_agreement/bbcagreement_july06.pdfhttp://www.bbc.co.uk/bbctrust/assets/files/pdf/regulatory_framework/charter_agreement/bbcagreement_july06.pdf

It proposes to measure the BBC's performance as follows:

"The Trust will measure: Audience perceptions of the BBC helping them to understand how to use new technology such as interactive TV and the internet. Qualitative audience research will also be used, particularly to explore how far audiences feel they have been helped to evaluate and engage with the many different sources of content available through digital media."

BBC sample projects

The BBC supports a broad range of activities aimed at developing media literacy. The projects listed below indicate the types of BBC activity directed at developing media literacy skills in relation to the internet.

The BBC has a long tradition of supporting computer users get online (starting with the BBC Micro in the late 1980s). **Webwise** began in the 1990s as a package to provide accessible routes to basic qualifications in using ICT. A network of centres was set up (for instance public libraries) where users could book in to specially run courses. Resources were also created online and these have been regularly updated. **Computer Tutor** was launched recently to provide entry level support for new computer users. It is video rich and designed for broadband delivery, and is targets at older users.

BBC News School Report gives 12 and 13-year-olds from UK schools the chance to make their own TV, radio or online news at school and to broadcast it for real. While the project is devised for this age group, students aged 11 to 14 may also take part. Using lesson plans and materials from the dedicated website, and with support from BBC staff, teachers help students develop their journalistic skills and become School Reporters.

BBC English Regions has made a huge commitment to media literacy over the last five years, particularly through its provision of 12 'learning buses' and open centres at 11 of its regional centres. Buses and Open centres ran a range of courses focusing on the internet, using computers and developing media skills more generally.

The Director-General informed the Trust that he has commissioned a major new online project which will enable the public to explore how contemporary media content is produced. The BBC believes this will be a major contribution to media literacy in Britain.

3.5 Media literacy and the Home Office

As part of its activity to protect children from potentially harmful or offensive content online the Home Office funds media campaigns in print, in cinemas and via broadcast media. These campaigns have been independently evaluated. The Home Office ran a campaign between September and November 2006 to support the roll-out of the Centre for Exploitation and Online Protection's (CEOP) *ThinkUKnow* schools programme. The online adverts were particularly successful, and have been seen by over 5.5 million unique visitors. *ThinkUKnow* was rolled out to Police Schools Liaison Officers and teachers beginning in September 2006. In October 2007 CEOP and Becta launched a "Cybercafe" where 8-11 year old children can learn about different aspects of online safety at their own pace.

Appendix 1: Privacy Policies for leading Social Networking Sites

1. Facebook[66]

Facebook Principles

We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.

Facebook follows two core principles:

1. You should have control over your personal information.
Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups you join. And you control the users with whom you share that information through the privacy settings on the My Privacy page.

2. You should have access to the information others want to share.
There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.

Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that information. If you have questions or ideas, please send them to privacy@facebook.com.

Safe Use of Facebook

For information for users and parents about staying safe on Facebook, click here.

Facebook's Privacy Policy

Facebook's Privacy Policy is designed to help you understand how we collect and use the personal information you decide to share, and help you make informed decisions when using Facebook, located at www.facebook.com and its directly associated domains (collectively, "Facebook" or "Website")

By using or accessing Facebook, you are accepting the practices described in this Privacy Policy.

Facebook is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build user's trust and confidence in the Internet by promoting the use of fair information practices. This privacy statement covers the site www.facebook.com and its directly associated domains. Because this Web site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe.

[66] http://www.facebook.com/policy.php

If you have questions or concerns regarding this statement, you should first contact our privacy staff at privacy@facebook.com. If you do not receive acknowledgement of your inquiry or your inquiry has not been satisfactorily addressed, you should contact TRUSTe Watchdog at http://www.truste.org/consumers/watchdog_complaint.php. TRUSTe will then serve as a liaison with us to resolve your concerns.

EU Safe Harbor Participation

We participate in the EU Safe Harbor Privacy Framework as set forth by the United States Department of Commerce. As part of our participation in the safe harbor, we have agreed to TRUSTe dispute resolution for disputes relating to our compliance with the Safe Harbor Privacy Framework. If you have any complaints regarding our compliance with the Safe Harbor you should first contact us at info@facebook.com. If contacting us does not resolve your complaint, you may raise your complaint with TRUSTe at http://www.truste.org/users/users_watchdog_intro.html.

The Information We Collect

When you visit Facebook you provide us with two types of information: personal information you knowingly choose to disclose that is collected by us and Web Site use information collected by us as you interact with our Web Site.

When you register with Facebook, you provide us with certain personal information, such as your name, your email address, your telephone number, your address, your gender, schools attended and any other personal or preference information that you provide to us.

When you enter Facebook, we collect your browser type and IP address. This information is gathered for all Facebook visitors. In addition, we store certain information from your browser using "cookies." A cookie is a piece of data stored on the user's computer tied to information about the user. We use session ID cookies to confirm that users are logged in. These cookies terminate once the user closes the browser. By default, we use a persistent cookie that stores your login ID (but not your password) to make it easier for you to login when you come back to Facebook. You can remove or block this cookie using the settings in your browser if you want to disable this convenience feature.

When you use Facebook, you may set up your personal profile, form relationships, send messages, perform searches and queries, form groups, set up events, add applications, and transmit information through various channels. We collect this information so that we can provide you the service and offer personalized features. In most cases, we retain it so that, for instance, you can return to view prior messages you have sent or easily see your friend list. When you update information, we usually keep a backup copy of the prior version for a reasonable period of time to enable reversion to the prior version of that information.

You post User Content (as defined in the Facebook Terms of Use) on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other Users with whom you may choose to share your pages and information. Therefore, we cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons. We are not responsible for circumvention of any privacy settings or security measures contained on the Site. You understand and acknowledge that, even after removal, copies of User Content may remain viewable in cached and archived pages or if other Users have copied or stored your User Content.

Any improper collection or misuse of information provided on Facebook is a violation of the Facebook Terms of Service and should be reported to privacy@facebook.com.

If you choose to use our invitation service to tell a friend about our site, we will ask you for information needed to send the invitation, such as your friend's email address. We will automatically send your friend a one-time email or instant message inviting him or her to visit the site. Facebook stores this information to send this one-time invitation, to register a friend connection if your invitation is

accepted, and to track the success of our referral program. Your friend may contact us at info@facebook.com to request that we remove this information from our database.

Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags) in order to provide you with more useful information and a more personalized experience.

By using Facebook, you are consenting to have your personal data transferred to and processed in the United States.

Children Under Age 13

Facebook does not knowingly collect or solicit personal information from anyone under the age of 13 or knowingly allow such persons to register. If you are under 13, please do not attempt to register for Facebook or send any information about yourself to us, including your name, address, telephone number, or email address. No one under age 13 may provide any personal information to or on Facebook. In the event that we learn that we have collected personal information from a child under age 13 without verification of parental consent, we will delete that information as quickly as possible. If you believe that we might have any information from or about a child under 13, please contact us at info@facebook.com.

Children Between the Ages of 13 and 18

We recommend that minors over the age of 13 ask their parents for permission before sending any information about themselves to anyone over the Internet.

Use of Information Obtained by Facebook

When you register with Facebook, you create your own profile and privacy settings. Your profile information, as well as your name, email and photo, are displayed to people in the networks specified in your privacy settings to enable you to connect with people on Facebook. We may occasionally use your name and email address to send you notifications regarding new services offered by Facebook that we think you may find valuable.

Profile information is used by Facebook primarily to be presented back to and edited by you when you access the service and to be presented to others permitted to view that information by your privacy settings. In some cases where your privacy settings permit it (e.g., posting to your wall), other Facebook users may be able to supplement your profile.

Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, network names, and profile picture thumbnail will be available in search results across the Facebook network and those limited pieces of information may be made available to third party search engines. This is primarily so your friends can find you and send a friend request. People who see your name in searches, however, will not be able to access your profile information unless they have a relationship to you (friend, friend of friend, member of your networks, etc.) that allows such access based on your privacy settings.

Facebook may send you service-related announcements from time to time through the general operation of the service. For instance, if a friend sends you a new message or poke, or someone posts on your wall, you may receive an email alerting you to that fact.

Generally, you may opt out of such emails here, though Facebook reserves the right to send you notices about your account even if you opt out of all voluntary email notifications.

Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are.

We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services, Facebook Platform developers and other users of Facebook, to supplement your profile. Where such information is used, we generally allow you to specify in your privacy settings that you do not want this to be done or to take other actions that limit the connection of this information to your profile (e.g., removing photo tag links).

Sharing Your Information with Third Parties

Facebook is about sharing information with others — friends and people in your networks — while providing you with privacy settings that restrict other users from accessing your information. We allow you to choose the information you provide to friends and networks through Facebook. Our network architecture and your privacy settings allow you to make informed choices about who has access to your information. We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you. For example:

- Your news feed and mini-feed may aggregate the information you provide and make it available to your friends and network members according to your privacy settings. You may set your preferences for your news feed and mini-feed here.
- Unlike most sites on the Web, Facebook limits access to site information by third party search engine "crawlers" (e.g. Google, Yahoo, MSN, Ask). Facebook takes action to block access by these engines to personal information beyond your name, profile picture, and limited aggregated data about your profile (e.g. number of wall postings).
- We may provide information to service providers to help us bring you the services we offer. Specifically, we may use third parties to facilitate our business, such as to host the service at a co-location facility for servers, to send out email updates about Facebook, to remove repetitive information from our user lists, to process payments for products or services, to offer an online job application process, or to provide search results or links (including sponsored links). In connection with these offerings and business operations, our service providers may have access to your personal information for use for a limited time in connection with these business activities. Where we utilize third parties for the processing of any personal information, we implement reasonable contractual and technical protections limiting the use of that information to the Facebook-specified purposes.
- If you, your friends, or members of your network use any third-party applications developed using the Facebook Platform ("Platform Applications"), those Platform Applications may access and share certain information about you with others in accordance with your privacy settings. You may opt-out of any sharing of certain or all information through Platform Applications on the Privacy Settings page. In addition, third party developers who have created and operate Platform Applications ("Platform Developers"), may also have access to your personal information (excluding your contact information) if you permit Platform Applications to access your data. Before allowing any Platform Developer to make any Platform Application available to you, Facebook requires the Platform Developer to enter into an agreement which, among other things, requires them to respect your privacy settings and strictly limits their collection, use, and storage of your information. However, while we have undertaken contractual and technical steps to restrict possible misuse of such information by such Platform Developers, we of course cannot and do not guarantee that all Platform Developers will abide by such agreements. Please note that Facebook does not screen or approve Platform Developers and cannot control how such Platform Developers use any personal information that they may obtain in connection with Platform Applications. In

addition, Platform Developers may require you to sign up to their own terms of service, privacy policies or other policies, which may give them additional rights or impose additional obligations on you, so please make sure to review these terms and policies carefully before using any Platform Application. You can report any suspected misuse of information through the Facebook Platform and we will investigate any such claim and take appropriate action against the Platform Developer up to and including terminating their participation in the Facebook Platform and/or other formal legal action.

- We occasionally provide demonstration accounts that allow non-users a glimpse into the Facebook world. Such accounts have only limited capabilities (e.g., messaging is disabled) and passwords are changed regularly to limit possible misuse.
- We may be required to disclose user information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards. Additionally, we may share account or other information when we believe it is necessary to comply with law, to protect our interests or property, to prevent fraud or other illegal activity perpetrated through the Facebook service or using the Facebook name, or to prevent imminent bodily harm. This may include sharing information with other companies, lawyers, agents or government agencies.
- We let you choose to share information with marketers or electronic commerce providers through sponsored groups or other on-site offers.
- We may offer stores or provide services jointly with other companies on Facebook. You can tell when another company is involved in any store or service provided on Facebook, and we may share customer information with that company in connection with your use of that store or service.
- Facebook Beacon is a means of sharing actions you have taken on third party sites, such as when you make a purchase or post a review, with your friends on Facebook. In order to provide you as a Facebook user with clear disclosure of the activity information being collected on third party sites and potentially shared with your friends on Facebook, we collect certain information from that site and present it to you after you have completed an action on that site. You have the choice to have Facebook discard that information, or to share it with your friends.
  To learn more about the operation of the service, we encourage you to read the tutorial here.
  To opt out of the service altogether, click here.
  Like many other websites that interact with third party sites, we may receive some information even if you are logged out from Facebook, or that pertains to non-Facebook users, from those sites in conjunction with the technical operation of the system. In cases where Facebook receives information on users that are not logged in, or on non-Facebook users, we do not attempt to associate it with individual Facebook accounts and will discard it.
- If the ownership of all or substantially all of the Facebook business, or individual business units owned by Facebook, Inc., were to change, your user information may be transferred to the new owner so the service can continue operations. In any such transfer of information, your user information would remain subject to the promises made in any pre-existing Privacy Policy.

When you use Facebook, certain information you post or share with third parties (e.g., a friend or someone in your network), such as personal information, comments, messages, photos, videos, Marketplace listings or other information, may be shared with other users in accordance with the privacy settings you select. All such sharing of information is done at your own risk. Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listings or other items , this information may become publicly available.

Links

Facebook may contain links to other websites. We are of course not responsible for the privacy practices of other web sites. We encourage our users to be aware when they leave our site to read the privacy statements of each and every web site that collects personally identifiable information. This Privacy Policy applies solely to information collected by Facebook.

Third Party Advertising

Advertisements that appear on Facebook are sometimes delivered (or "served") directly to users by third party advertisers. They automatically receive your IP address when this happens. These third party advertisers may also download cookies to your computer, or use other technologies such as JavaScript and "web beacons" (also known as "1x1 gifs") to measure the effectiveness of their ads and to personalize advertising content. Doing this allows the advertising network to recognize your computer each time they send you an advertisement in order to measure the effectiveness of their ads and to personalize advertising content. In this way, they may compile information about where individuals using your computer or browser saw their advertisements and determine which advertisements are clicked. Facebook does not have access to or control of the cookies that may be placed by the third party advertisers. Third party advertisers have no access to your contact information stored on Facebook unless you choose to share it with them.

This privacy policy covers the use of cookies by Facebook and does not cover the use of cookies or other tracking technologies by any of its advertisers.

Changing or Removing Information

Access and control over most personal information on Facebook is readily available through the profile editing tools. Facebook users may modify or delete any of their profile information at any time by logging into their account. Information will be updated immediately. Individuals who wish to deactivate their Facebook account may do so on the My Account page. Removed information may persist in backup copies for a reasonable period of time but will not be generally available to members of Facebook.

Where you make use of the communication features of the service to share information with other individuals on Facebook, however, (e.g., sending a personal message to another Facebook user) you generally cannot remove such communications.

Security

Facebook takes appropriate precautions to protect our users' information. Your account information is located on a secured server behind a firewall. When you enter sensitive information (such as credit card number or your password), we encrypt that information using secure socket layer technology (SSL). (To learn more about SSL, go to http://en.wikipedia.org/wiki/Secure_Sockets_Layer). Because email and instant messaging are not recognized as secure communications, we request that you not send private information to us by email or instant messaging services. If you have any questions about the security of Facebook Web Site, please contact us at privacy@facebook.com

Terms of Use, Notices and Revisions

Your use of Facebook, and any disputes arising from it, is subject to this Privacy Policy as well as our Terms of Use and all of its dispute resolution provisions including arbitration, limitation on damages and choice of law. We reserve the right to change our Privacy Policy and our Terms of Use at any time. Non-material changes and clarifications will take effect immediately, and material changes will take effect within 30 days of their posting on this site. If we make changes, we will post them and will indicate at the top of this page the policy's new effective date. If we make material changes to this policy, we will notify you here, by email, or through notice on our home page. We encourage you to refer to this policy on an ongoing basis so that you understand our current privacy policy. Unless stated otherwise, our current privacy policy applies to all information that we have about you and your account.

Contacting the Web Site

If you have any questions about this privacy policy, please contact us at privacy@facebook.com. You may also contact us by mail at 156 University Avenue, Palo Alto, CA 94301.

2. MySpace[67]

About MySpace.com

MySpace.com is an online service that allows our members to set up unique personal profiles that can be linked together through networks of friends. MySpace members can view each others' profiles, communicate with old friends and meet new friends on the service, share photos, post journals and comments, and describe their interests. To enrich our members' experience, we request and display some personal information to other members and visitors, which allows our users to identify each other and expand their network of friends. MySpace members can change their profile information at any time and can control how other members and the service communicates with them.

MySpace.com cares deeply about online privacy If you have any questions concerning this privacy policy, please email us at privacy@myspace.com.

Information Collection and Use by MySpace.com

MySpace.com collects user submitted information such as name, email address, and age to authenticate users and to send notifications to those users relating to the MySpace.com service. MySpace.com also collects other profile data including but not limited to: personal interests, gender, age, education and occupation in order to assist users in finding and communicating with each other.

MySpace.com also logs non-personally-identifiable information including IP address, profile information, aggregate user data, and browser type, from users and visitors to the site This data is used to manage the website, track usage and improve the website services. This non-personally-identifiable information may be shared with third-parties to provide more relevant services and advertisements to members. User IP addresses are recorded for security and monitoring purposes

User Profile information including members' pictures and first names are displayed to people in order to facilitate user interaction in the MySpace.com social networking community. Email addresses are used for the purposes of inviting new friends to join MySpace, to add users to members' friends' networks, and to send notifications related to the service. With the exception of inviting friends, adding friends, and notifications, a user's email address is not shared or displayed to people within a user's personal network Users within a personal network communicate on MySpace.com with each other through the MySpace.com service, without disclosing their email addresses. Users' full names are never directly revealed to other members. To facilitate searching and finding friends and acquaintances on the service, MySpace.com allows users to search for other members using first and last name, email address, and schools and/or companies where users may have attended or worked.

We may also use a user's email address to send updates, a newsletter or news regarding the service. Users may choose not to receive email of this type by changing their "notification" setting to "Do not send me notification emails" in the user "Account Settings"

From time to time, MySpace.com or a partner, may sponsor a promotion, sweepstake or contest on myspace.com. Users may be asked to provide personal information including name, email address or home address or to answer questions in order to participate. We may transfer personal information to certain ad partners that you have explicitly requested to receive information from. It will be clear at the point of collection who is collecting the personal information and whose privacy statement will apply.

Invitations and Other Communications to Non-members

MySpace members can invite friends to join the service by sending invitation emails via our automated invitation system. MySpace.com stores the email addresses that members provide so that the respondents may be added to the friend's list of the member sending the invitations, and also to send reminders of the invitations MySpace.com does not sell these email addresses or use them to send any other communication besides invitations, invitation reminders (up to three (3) per email address). Recipients of invitations from MySpace.com may contact MySpace.com to request the removal of their information from our database.

[67] http://www.myspace.com/index.cfm?fuseaction=misc.privacy

MySpace members may also store email addresses of people they know in their internal MySpace address book and may also choose to send invitations and other communications to those addresses.

You may prevent MySpace.com email invitations and other messages from being sent to any email address you control by sending a single email with the subject "BLOCK" to privacy@myspace.com Please note that the email must come from the account you wish to block.

Use of Cookies

MySpace.com uses cookies to store visitors' preferences and to record session information, for purposes including ensuring that visitors are not repeatedly offered the same advertisements and to customize newsletter, advertising, and Web page content based on browser type and user profile information. We do not link the information we store in cookies to any personally identifiable information you submit while on our site. You may be able to configure your browser to accept or reject all or some cookies, or notify you when a cookie is set -- each browser is different, so check the "Help" menu of your browser to learn how to change your cookie preferences -- however, you must enable cookies from MySpace.com in order to use most functions on the site Please note that MySpace allows 3rd party advertisers that are presenting advertisements on some of our pages to set and access their cookies on your computer. Advertisers' use of cookies is subject to their own privacy policies, not the MySpace Privacy Policy.

Links

MySpace.com contains links to sites. MySpace.com is not responsible for the privacy policies and/or practices on other sites. When linking to another site a user should read the privacy policy stated on that site. Our privacy policy only governs information collected on MySpace.com.

Chat Rooms, Journals and WebLogs, Message Boards, Classifieds and Public Forums

Please be aware that whenever you voluntarily post public information to Journals, WebLogs, Message Boards, Classifieds or any other Public Forums that that information can be accessed by the public and can in turn be used by those people to send you unsolicited communications.

Correcting/Updating or Removing Information

MySpace.com users may modify or remove any of their personal information at any time by logging into their account and accessing features such as Edit Profile and Account Info.

Email Choice/Opt-out

Members who no longer wish to receive updates or notifications may choose not to by selecting 'Do not send me notification emails' in the user profile 'Account Settings'. Users who do not wish to receive MySpace.com newsletters may choose not to by selecting 'Do not send me MySpace newsletters' in the user profile 'Account Settings'. All notification emails and MySpace.com newsletters also include the above instructions for opting-out of those communications in the future.

Third Party Advertising

Ads appearing on this Web site may be delivered to users by MySpace.com or one of our Web advertising partners. Our Web advertising partners may set cookies. These cookies allow the ad server to recognize your computer each time they send you an online advertisement. In this way, ad servers may compile information about where you, or others who are using your computer, saw their advertisements and determine which ads are clicked on. This information allows an ad network to deliver targeted advertisements that they believe will be of most interest to you. This privacy statement covers the use of cookies by MySpace.com and does not cover the use of cookies by any advertisers.

Security

MySpace.com member accounts are secured by member-created passwords MySpace.com takes precautions to insure that member account information is kept private. We use reasonable measures to protect member information that is stored within our database, and we restrict access to member information to those employees who need access to perform their job functions, such as our customer service personnel and technical staff. Please note that we cannot guarantee the security of member account information. Unauthorized entry or use, hardware or software failure, and other factors may

compromise the security of member information at any time For any additional information about the security measures we use on MySpace.com, please contact us a privacy@myspace.com

Sharing and Disclosure of Information MySpace.com Collects

Except as otherwise described in this privacy statement, MySpace will not disclose personal information to any third party unless we believe that disclosure is necessary: (1) to conform to legal requirements or to respond to a subpoena, search warrant or other legal process received by MySpace.com, whether or not a response is required by applicable law; (2) to enforce the MySpace.com Terms of Use Agreement or to protect our rights; or (3) to protect the safety of members of the public and users of the service. MySpace reserves the right to transfer personal information to a successor in interest that acquires rights to that information as a result of the sale of MySpace or substantially all of its assets to that successor in interest For more information see the "Changes in Our Privacy Policy" section below.

Changes in Our Privacy Policy

From time to time we may make changes to our privacy policy If we make changes, we will post them on our site to make users aware of what the changes are so users will always be aware of what information we collect, how we use it, and when we may disclose it. A User is bound by any minor changes to the policy when she or he uses the site after those changes have been posted If, however, we are going to use users' personally identifiable information in a manner materially different from that stated at the time of collection we will notify by posting a notice on our Web site for 30 days.

Contacting the Web Site

If you have any questions about this privacy statement, the practices of this site, or your dealings with this Web site, please contact us at: privacy@myspace.com (8391 Beverly Blvd, #349, Los Angeles, CA 90048)

3. bebo

Privacy Policy[68]

Updated: November 29, 2007

Our Commitment to You

Welcome to Bebo.com, the next generation social networking site where members can stay in touch with their friends, meet new people and hang out. The founders and employees of Bebo take your privacy very seriously. To make it easier for you to read and understand our privacy policy, we did the unconventional thing -- we wrote it in plain English and tried to keep it to a reasonably short length.

The key points of our privacy policy are:

- Your privacy remains under your control.
- You can end your membership at any time.
- We only disclose information from which you may be personally identifiable to selected third parties in accordance with this privacy policy.
- Bebo does not spam.
- By participating in the Bebo community, you agree to this privacy policy.

Information collected by Bebo

We collect the following types of information about you when you use Bebo:

- Information provided by you. We collect personal information, such as your name and email address, when you register to become a member of Bebo.com. This information is used when you set up your personal profile. As part of your personal profile, you may choose to submit additional information such as your age, your hobbies and interests and other content, such as photos, music and videos.
- Information collected automatically. Bebo receives and stores information which is transmitted automatically from your computer when you browse the Internet and use Bebo. This information includes information from cookies (which are described in paragraph 4 below), your IP address and browser type. Your IP address is the unique address of your computer which is automatically provided to other computers when your web browser or email application requests a web page or email from those computers on the Internet.

Use and Disclosure of information

- We will display your personal information on your profile according to the preferences you set. We will use your name so that you are recognisable on our database and so that we can personalize your experience. We will use your email address to contact you from time to time and may also use it for security reasons to confirm that you are who you say you are. You can control the types and frequencies of certain emails you receive in your email preferences.
- We may use the information collected automatically, such as your IP address and information stored via cookies, to gather statistics about the number of people who visit Bebo and to customise Bebos content, layout and services. We may share this information with third parties to help us improve Bebo and better serve our users.

[68] http://www.bebo.com/Privacy.jsp

- Advertisements that appear on Bebo are delivered to you by our advertising partners. Bebo may transfer information about your use of Bebo, such as your IP address and information stored via cookies, to our advertising partners (including Yahoo! and its affiliates) and other third parties. This information may be used to provide advertising, promotions and other products and services that may be of particular interest to you. It may also be used to provide you with a tailored choice of content and media products. If you do not want to receive targeted advertisements at any point in the future, please change your advertisement preferences in your account or send a request to us via the Contact Us page.
- Our advertising and promotions partners have no access to your name or personal contact information stored by Bebo unless you choose to share it with them. Bebo does not provide your name or personal contact information to an advertising partner when you interact with or view a targeted advertisement.
- We may provide your personally identifiable information and the data generated by cookies and the aggregate information to the vendors and service agencies that we may engage to assist us in providing our services to you. Such third party entities will be obligated to use your personally identifiable information solely to provide the services to us.
- We will disclose your personally identifiable information if we reasonably believe we are required to do so by law, regulation or other government authority or to protect the rights and property of Bebo.com, its affiliates or the public. We may also co-operate with law enforcement agencies in any official investigation and we may disclose your personally identifiable information to the relevant agency or authority in doing so.
- We reserve the right to transfer your personal information in the event of a transfer of ownership of Bebo.com, such as acquisition by or merger with another company. If an acquiring company should plan to materially change this privacy policy, we will notify you beforehand.

Tell-A-Friend

If you choose to use our referral service to tell a friend about Bebo, we will ask you for your friends name and email address. We will automatically send your friend a one-time email inviting him or her to visit Bebo. Bebo stores and only uses this information for the sole purpose of sending this one-time email and tracking the success of our referral program.

Your friend may submit a request that we remove this information from our database via the Contact Us page or by emailing customerservice@bebo.com; remove requests of this nature will be completed within 30 days.

Links to Other Sites

This Web site contains links to other sites that are not owned or controlled by Bebo. Please be aware that we, Bebo, are not responsible for the privacy practices of such other sites.

We encourage you to be aware when you leave our Web site and to read the privacy statements of each and every site that collects personally identifiable information.

This privacy statement applies only to information collected by this Web site.

"Masking" is a function of using programming techniques such that the displayed URL does not match the actual pages being viewed (e.g. user is on www.xyz.com, but the URL displayed is www.abc.com). In certain circumstances, Bebo may use Masking and, although it will appear that you are still on the Bebo Web site, you may be on a different site. For example, when you create a widget or when you upload a video, you may be transferred to a third party's site and the privacy policy of the applicable third party site applies.

Testimonials

We post customer testimonials on our Web site which may contain personally identifiable information such as your name. We obtain your prior consent to post your name along with your testimonial.

Cookies

- Cookies are a common Internet technology. Many web sites use cookies to provide useful features for their users. Cookies are small files that are written or downloaded to your computers hard drive when you access a site. They allow Bebo to store and quickly retrieve login information on your computer and provide data that we can use to improve the quality of our service. Most Internet browsers (such as Internet Explorer and Safari) are initially set up to accept cookies. If you prefer, you can set your browser to refuse cookies, although you may not be able to take full advantage of Bebo if you do so. You can disable cookies by going to Tools on your top menu bar. This will bring up the "Internet Options" dialogue box. On the top of the dialogue box, click on "Privacy". This will bring up the "Settings" box. Scroll up using the slide bar on the left-hand side of the box, until the wording in the box states Block All Cookies. Then click on the "OK" button on the bottom of the menu box. If you follow these instructions, your computer will not accept cookies in future.
- Bebo may link information stored in cookies such as your age, gender and country with your personally identifiable information and we may use such information to gather statistics about the number of people who visit Bebo and to customize Bebos content, layout and services for delivery to you.
- Our advertising partners may set and access cookies or use other technologies such as web beacons (which are electronic files that allow a web site to count users who have visited that page or to access certain cookies) in order to personalise advertising content. Use by these advertising partners of their own cookies and any other tracking technologies are subject to their privacy policies. Bebo uses its reasonable efforts to ensure that its advertising partners are operating privacy policies that are in accordance with Bebos own privacy standards as set out in this privacy policy.

You control who shares your information

- Your Bebo profile information will only be shared with people you have specifically agreed to share such information with, and to other members of groups (such as universities) you choose to belong to. You can limit who can view certain personal information, such as email addresses and phone numbers. Please bear in mind that if you choose to share your personal information (including any comments, videos, photos or any other information) to other people on Bebo, you do so at your own risk. Bebo recommends that you dont share your personal contact information.
- You can choose to make your profile visible to non-members of Bebo by editing your profile and opting in to accessible profile.

Reviewing, deleting and changing your Profile

You can review, delete, correct and revise your privacy settings and personal profile, including who has access to your personal profile in your account at any time or contact us for assistance via the Contact Us page or via email to customerservice@bebo.com; requests of this nature will be completed within 30 days.

Internet awareness

Whenever you voluntarily post personal information in public areas, like journals, weblogs, message boards and forums, this information can be accessed by the public and can in turn be used by others to send you unsolicited communications. Bebo recommends that you exercise discretion in deciding what information you disclose on the Internet.

Children

- Children under the age of 13 are not eligible to use Bebo and must not attempt to register with Bebo and/or submit any personal information to us. Bebo does not knowingly collect personal information from any person who is under the age of 13 or allow them to register. If it comes to our attention that we have collected personal data from a person under the age of 13, we

will delete this information as quickly as possible. If you have reason to believe that this has occurred, please contact us via the Contact Us page, and we will delete any such information.

- We recommend that children between the ages of 13 and 17 should not send any information about themselves to anyone over the Internet without asking their parents or legal guardians for permission beforehand. Bebo is a member of the working party involved in the drafting of the UK Home Offices Good practice guidance for the providers of social networking and user interactive services 2007.

Security and confidentiality

- The security of your personal information depends on your protection of your account password. Please do not disclose your account password to unauthorized people. Bebo uses industry standard technology designed to help keep your personal information safe. Please bear in mind though, that it is impossible for Bebo to guarantee that impenetrable security measures are in place. For example, we cannot control any illegal and/or unforeseen activity of other users that may allow them to get around the privacy or security settings on the Bebo website. Consequently, you acknowledge that there are circumstances in which your personal information may be accessed by unauthorised persons.
- We limit access to your personal information only to employees who we believe need to come into contact with that information in order to do their jobs in connection with the Bebo service.
- If you become aware of any breach of data security or have any other questions about the security of our website, please contact us via the Contact Us page.

Changes in Privacy Policy

If we decide to change our privacy policy, we will post those changes to this privacy statement, the home page, and other places we deem appropriate so that you are aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it.

We reserve the right to modify this privacy statement at any time, so please review it frequently. If we make material changes to this policy, we will notify you here, by email, or by means of a notice on our home page.

Additionally, we may send registered users an email notifying you of the change. IF ANY MODIFICATION IS UNACCEPTABLE TO YOU, YOU SHALL STOP USING THE BEBO SERVICE. YOUR CONTINUED USE OF THE BEBO SERVICE FOLLOWING OUR POSTING OF A CHANGE NOTICE OR ON OUR WEBSITE OR BLOG OR RECEIVING OUR EMAIL NOTIFYING YOU OF THE CHANGE WILL CONSTITUTE YOUR BINDING ACCEPTANCE OF THE CHANGE.

Canceling membership

You always have the option to cancel your membership at any time. If you are a member and no longer wish to participate in Bebo you can sign in to the site and click on the My Account at the top of the page; then select cancel membership and follow the simple instructions.

Co-Branding

The Bebo Web site may be co-branded with our partners, such as Oracle and Yahoo search.

Contact and TRUSTe

Bebo is a licensee of the TRUSTe Web Privacy Seal Program. TRUSTe is an independent, non-profit organization whose mission is to build users trust and confidence in the Internet by promoting the use of fair information practices. This privacy statement covers the Web site www.bebo.com. Because this Web site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe.

Bebo abides by the EU Safe Harbor framework as set forth by the Department of Commerce regarding collection, use, and retention of data from the European Union.

If you have questions or concerns regarding this statement, you should first contact us on the Contact Us page or write to:

Customer Support
Bebo, Inc.
795 Folsom St, 6th Floor
San Francisco
CA 94107
USA

or via email to customerservice@bebo.com.

If you do not receive acknowledgement of your inquiry or your inquiry has not been satisfactorily addressed, you should contact TRUSTe at http://www.truste.org/consumers/watchdog_complaint.php TRUSTe will then serve as a liaison with us to resolve your concerns.

Effective Date and Last Revision Date

This Privacy Policy was first posted on July 15, 2005

This Privacy Policy was last revised and is effective as of November 29, 2007