OFFICE OF COMMUNICATIONS

Ofcom's Response to the Byron Review

Statement

Publication date: March 27 2008

Contents

Foreword

The past decade has seen significant changes in the communications and broadcasting landscape. Children and young people are at the forefront of these changes: as our research shows, they are some of the heaviest users of new media, from text messaging to MP3 players, games consoles and the internet. The internet in particular offers rich opportunities for them to learn, to get help with their education and to enrich their communications with family and friends, amongst others. But the internet also presents challenges, particularly to their safety and wellbeing, arising from exposure to potentially harmful or inappropriate material.

So we welcome the Byron Review and the opportunity it affords for a timely and balanced discussion of the issues. We believe the Review will inform and stimulate an evidence-based debate with industry, government and consumers about the possible range of activities to help address these real concerns.

In particular, we welcome the opportunity to begin the discussion about how best to secure consumer protections in the online age in the online age. At a time of sweeping change in content delivery, and in the type of content that is available, the overall goals of content regulation persist. These are to ensure that people have the information and skills they need to take responsibility for their media choices. In linear broadcasting, the schedule and the watershed are powerful and well understood tools for signalling the characteristics of content to audiences. Our aim must now be to help inform consumers for the online world.

Although the goals are the same, the broadcast model of content regulation is not appropriate for potentially harmful online content. Rather, a new approach to content regulation is required: one which is built on a model of shared responsibility, which gives people the tools they need to take personal responsibility and which supports effective industry self-regulation. The growing importance of online media literacy derives from this: media-literate parents and children, equipped to take on this personal responsibility, provide a significant means of protection.

Ofcom's research, analysis and experience lead us to believe at this stage that this approach is the likeliest to be successful, and to build confidence for children, young people, their parents, and wider society.

We look forward to the outcomes of the review, and to working with all sectors of industry and consumer groups to achieve these goals.

David Currie **Ed Richards**

Section 1

Introduction

Ofcom is pleased to submit its response to the call for evidence issued by the Byron Review team on October 9th 2007. We welcome in particular the opportunity to have a balanced, evidence-led discussion about:

- the benefits of the internet;
- the potential or actual risks to children's safety and wellbeing arising from exposure to potentially harmful or inappropriate material on the internet; and
- the effectiveness and adequacy of existing measures to help prevent children from being exposed to such material and to help parents understand and manage the risks of access to inappropriate content.

The key questions for the review are:

- What are the benefits and opportunities that new technologies offer for children, young people, their families, society and the economy?
- What are the potential or actual risks to children's safety and wellbeing of going online and playing video games and how do children, young people and parents feel about those risks?
- To what extent do children, young people and parents understand and manage those risks and how can they be supported to do so?
- What, if anything, could be changed in order to help children, young people and parents manage the potential or actual risks of going online or playing video games, and what are the pros and cons of different approaches?

Our submission focuses primarily on children's home PC/laptop internet experience, although, where appropriate, we also make reference to their mobile phone internet use and/or their online gaming experience.

Section 3 of the Communications Act 2003 ("the Act") sets out Ofcom's principal duties in carrying out its functions are to further the interests of citizens in relation to communication matters and to further the interests of consumers in relevant markets, where appropriate by promoting competition. While Ofcom's statutory duties as a content regulator are exclusively directed to TV and Radio broadcasting we also have legal responsibilities in respect of internet connectivity. We also have a statutory duty to promote media literacy (Section 11 of the Act) – a role in encouraging consumers to make the most of services on the internet, and to learn how to manage the risks to which they are exposed when online. We therefore have an interest in the protection of consumers from harm when they use the internet.

In preparing our submission we considered the following areas, each of which is provided as an annex to this document:

- **How does the internet work? (Annex 1)**

Provides an overview of the internet value chain, the different types of content and services available on the internet, the economics of the internet and the key players.

- **Current tools and approaches to regulating the internet (Annex 2)**

  Outlines the current regulatory thinking, the legal and regulatory structures in the UK, and the initiatives that are already under way at different points in the online content value chain.

- **TV Content regulation and child protection: policy, practice and user tools (Annex 3)**

  Summarises the current legal and regulatory structures for TV and points to the lessons that can be learned from TV content regulation; provides an overview of the Audio Visual Media Services Directive (AVMS).

- **Online child protection - the international perspective (Annex 4)**

  Reviews approaches adopted in five other countries: France, Germany, Australia, the US and South Korea. We also take a brief look at the approaches taken in China and Saudi Arabia.

- **The research evidence base: the views of children, young people and parents (Annex 5)**

  Here we summarise the findings from the 'Children, Young People and Online Content' research that was commissioned to provide us with up-to-date feedback on this topic from parents, children and young people[1]. We also refer to other Ofcom research, as well as to other publicly available research, as appropriate.

- **Harm and offence in media content: updating the 2006 review (Annex 6)**

  Ofcom commissioned Sonia Livingstone and Andrea Millwood Hargrave to update the literature review on Harm and Offence in Media Content, first published in 2006. The updated literature review focuses on TV, games, the internet and mobiles.

We have structured our submission as follows:

Chapter 2 is an executive summary of chapters 3-6.

Chapter 3 looks at the benefits and opportunities that the internet offers for children, young people, their families, society and the economy.

Chapter 4 addresses the views of parents, children and young people about children's and young people's use of the internet and the potential or actual risks to children's safety and wellbeing in going online.

[1] Between October 25 and November 7 TNS (the market research agency) conducted face-to-face, computer aided interviews with 653 parents, 653 children aged between 5-17 years from the same household, and 279 non-parents. We use the phrase "young people" to refer specifically to 16-17 year-olds. When we refer to the full sample of children aged 5-17, we use the phrases "children" or "children and young people" interchangeably, The interviews covered: current media habits and consumption, attitudes to the internet, parental rules around internet use, use of and satisfaction with software filters, concerns about the internet and mobile internet, exposure to inappropriate material online and awareness of who to complain to. We deliberately interviewed a parent and child from the same household so that we could directly compare their responses.

Chapter 5 summarises the conclusions of a review of the literature on the risks of harm to children from exposure to inappropriate content.

Finally, **Chapter 6** considers what could be changed in order to help children, young people and parents manage the potential or actual risks of going online, as well as the pros and cons of different approaches. It is in this context that we recommend options for the Byron Review team's further consideration.

This body of current evidence and analysis has informed the recommendations we have made; however, the fast pace of development in the online environment means that we must remain open to new evidence and to alternative ways to address the potential risks we have identified.

Section 2

Executive summary

The internet is much used and valued by children, young people and parents, and the importance of the internet to the child increases with age.

Overall, 99% of children aged 8-17 say that they use the internet, and 80% of households with children aged 5-17 have internet access at home (compared to 57% of households without children)2.

While TV remains the dominant medium for children aged 5-15, the use and importance of the internet to the child increases with age, both in terms of hours of use and in its status as the medium the child would miss the most.

Average hours of use of the internet have increased greatly over the past two years (from 7.1 hours/week in 2005 to 13.8 hours/week in 2007 for 12-15 year-olds).

The uses made of the internet by children vary considerably by age: younger children tend to use it more to play games, older children as an educational tool as well as for searching, email, watching or downloading video clips, and using social networking sites.

A mixed picture emerges regarding the degree and effectiveness of parental oversight of internet use at home.

For a start, one of the challenges faced by parents is that almost half (47%), believe their child is more skilled at using the internet than they are. This is especially true of the parents of older children (61% of parents of 12-17 year olds).

There are also differences in what parents and young people say about the presence of 'internet rules' at home: the research indicates that parents tend to claim greater presence and use of these rules compared to children, especially in the case of children under 15.

Just over half of parents said that they had content filtering software installed; a further 9% said that they had not heard of filtering (until now) but would be interested in using it in the future. Around one in five was familiar with content filtering software, but did not use it, with the reason most frequently given being because they trusted their children. This suggests that parents think that this type of software is used to prevent children from accessing certain types of content rather than as a tool which could be used to help provide protection from such material. Other reasons mentioned were that their children were too young to surf the web/use the internet, or because they did not think they needed it.

While parents generally seem to have a good understanding of the uses their child makes of the internet at home, there are some notable exceptions: they seem to be underestimating, in particular: game playing, watching video clips, using social networking sites and contributing comments to someone else's web page. This is borne out, for example, by the finding that around one in five parents do not know if their child has a social networking site profile.

One possible reason for this is unsupervised use; overall, 16% of children have a computer with internet access in their bedroom (this rises from 1% of 5-7 year olds, to 12% of 8-11

[2] See Annex 5 for the full research report and a methodological overview.

year olds and 24% of 12-17 year olds); parents also tend to underestimate their child's access to the internet at a friend's house.

Finally, while the majority of parents believe that they have done what needs to be done to help their child stay safe when online, there is a sizeable group of parents (over one in four) who say that they do not have any rules in place.

This points to, on the one hand, a group of parents who may not be doing enough to ensure that their children are safe online, and, on the other hand, to another group who have rules in place, but where there are potential shortfalls in the effectiveness of these rules.

While almost one in seven 8-17 year-olds say they have come across potentially harmful or inappropriate material in the past six months, almost one in ten parents[3] do not know if their children have or not. The likelihood of coming across such material increases with the age of the child, as does the likelihood of the parent not knowing if the child has done so.

While the majority of children and parents agree that the child would tell the parent if they came across something that worried them, this does not always seem to be the case: overall, 16% of 8-17 year-olds say they have come across harmful or inappropriate material[4] in the past six months, while 12% of parents with children in this age group say that their child has; almost one in ten parents (8%) do not know if their child has come across harmful or inappropriate content in the past six months.

Responses from parents and children indicate that most of this material was seen at home, but children also say that they have seen it at school or at friends'/relatives' houses. Parents seem to be less aware of out-of-home exposure to potentially harmful or inappropriate content. This clearly has implications for the impact of their rules on the child's levels of potential exposure and risk.

Sexual content is by far the most frequently mentioned type of potentially harmful or inappropriate content, followed by violence and pop-up adverts with harmful or inappropriate content.

Most children say that they leave the site when they come across such material, with only a small percentage saying that they tell a parent (possibly because they are not sufficiently concerned or worried about it).

The majority of parents (57%) do not know where to go to get information about how to help protect their children online.

Between 5% and 8% mentioned other websites, schools, family/friends/colleagues, or the library; 3% or fewer mentioned *Get Safe Online*, *ThinkYouKnow,* the Internet Watch Foundation, the Citizens' Advice Bureau or CEOP (Child Exploitation and Online Protection).

A substantial minority of parents – almost four in ten – would not know who to complain to if they came across something potentially harmful or inappropriate.

[3] Parents of children aged 8-17

[4] We asked first of all if they had come across harmful or inappropriate material in the past 6 months and, if they had, we asked the open-ended question 'What type of content was it?'. Thus these findings relate to self-reported harmful or inappropriate material.

Around a third would complain to the police, 14% to their ISP and 11% to the websites themselves. Most children say they would complain to their parents (though whether they would or not is questionable, given the findings reported above).

Although parents and children do have concerns about the internet, for both, the benefits outweigh the risks.

In research conducted for this submission, the vast majority of parents agreed that online children discover interesting, useful things that they did not know before, and both parents and children overwhelmingly agreed that the internet helps children with school/college work.

Almost two-thirds of the parents and children interviewed in this research agreed that children who do not have/use the internet are at a disadvantage.

The majority of parents agreed that they trusted their child to use the internet safely, and that it was safe for them to go online; in general, the children interviewed were more confident of their ability to manage online risk than their parents were.

While the majority of parents clearly have concerns about the internet (66% of all parents have concerns), the reverse is true of children (30% of 8-17 year olds have concerns). Parents have concerns about risks on the internet (especially regarding sexual content, paedophiles masquerading as children, child abuse imagery and bad language).

While parents overwhelmingly believe that internet users must be protected from seeing inappropriate or offensive content, slightly more than half agree that internet sites must be free to be expressive and creative.

Finally, a majority of parents think that the benefits of the internet outweigh the risks, and that real-life concerns like bullying and violence are more worrying. Children in particular agree with the latter statement.

Does exposure to potentially harmful or inappropriate material lead to actual harm? We commissioned Sonia Livingstone and Andrea Millwood Hargrave to update their 2005 literature review: *Harm and Offence in the Media*[5]. In brief, the literature review identifies evidence suggesting some risk of harm. However, the evidence base is patchy and undeveloped and, for both practical and ethical reasons, some key questions remain difficult to research; the evidence that does exist points to the increased potential for harm online. Therefore research can only guide policy by supporting a judgement based on the balance of probabilities rather than on irrefutable proof.

The research findings reported above, and the overall conclusions from the literature review, suggest a lack of evidence for actual harm, but evidence for the risk of harm. We can conclude from this that there is a case for considering what could be done to help children and parents manage the potential or actual online risks.

For the internet, there is no single institution which can do what the broadcast TV channel does (i.e. assume responsibility for content standards). Instead, we believe that responsibility is shared, or distributed, across the system: players across the internet value chain all have a role to play in mitigating the risk of harm.

Below we outline our thoughts on proportionate ways in which the potential risks can be managed. In developing these recommendations we considered the extent to which action

[5] See Annex 6 for the full report: Harm and Offence in Media Content: Updating the 2005 Review; Millwood Hargrave, A., Livingstone, S., with Brake, D.

was needed at all (the 'do nothing' option); and the extent to which direct statutory intervention might be the appropriate way of addressing parental concerns and the potential for harm, supported by our research. We conclude that current legal constraints and the problems of jurisdictional reach make statutory regulation impractical and, even if it were adopted as an approach, it may be of limited effectiveness. This is, in large part, because the internet is an open, global platform, and statutory regulation can only have national reach – unless the regulation also involves curtailing this openness and global reach, which distinguish the internet from traditional platforms and in many respects are the basis of its impact and value.

Instead, a new approach to content regulation is needed, one which is built on a model of responsibility distributed across the value chain, relying much more on personal responsibility and on industry self-regulation than on traditional, formal intervention.

In order to help people take more personal responsibility when they go online, we need to help them become more media literate. Media literacy is the ability to access, understand and create communications in a variety of contexts. Some call this 'literacy for the twenty-first century'. Put another way, if literacy is not only about reading and writing, but also about comprehension and critical thinking, then media literacy is about engaging these capabilities when using and consuming media. Without media literacy, people's ability to participate effectively in society, the marketplace and in the workforce may be greatly diminished. The remit of the Byron Review focuses principally on issues related to access – how to find the content and services wanted and how to avoid the content which may be potentially harmful or offensive – and indeed this is the focus of our response. However, Ofcom also recognises the importance of 'understanding' and 'creating' in the broader media literacy landscape, and these latter aspects are a part of our overall media literacy work programme.

We believe that both of these elements – greater media literacy on the part of parents, young people and children, coupled with targeted industry support – are critical and necessary in order to deliver a safer online environment for children. We look at each element in turn below.

Personal responsibility - media literacy: parents, children and young people

The evidence clearly points to a need to help parents, children and young people manage the potential or actual risks of going online by improving their media literacy skills. We suggest a focus on the following media literacy outcomes to help parents, children and young people manage the potential or actual risks of going online:

Outcomes

- Increased awareness and understanding among parents of their critical role in ensuring the safety of their children when they are online, through the effective application of carefully targeted and age-appropriate rules.
  For example:
  - Increased parental awareness of where to go to get information on protecting their child online as well as tips to ensure that the child has understood and accepted the importance of any rules that the parent puts in place (e.g. an internet green cross code).
  - Increased parental understanding of how they can apply their real-world parenting skills to the online world (i.e. it's not necessarily just about technical literacy).

- Increased parental awareness of what children are doing online more generally and the key areas/things that they need to look out for.

- Increased awareness of the age-appropriateness of certain activities online, e.g. using a social networking site (SNS).

- Increased parental and children's awareness of the risks of children's content access and other online activity (e.g. privacy in relation to the personal information that children share about themselves online) as well as child contact.

- Increased awareness of where to find high-quality content online, for younger children in particular.

- Increased take-up of content management tools such as filtering software, by making parents aware both of its existence, its benefits and its limitations.

    - Increased use of other forms of filtering, such as those provided by search engines.

    - Increased awareness and understanding of the tools provided by parents' Internet Service Providers (ISPs) and awareness of those ISPs which are more 'family-friendly'; for example, as demonstrated by the presence of a family-friendly 'trustmark'.[6]

- Increased awareness and understanding of the meanings of the content labels used by industry, as well as the implications of these in relation to children's use of content.

- Increased awareness of where to complain about potentially harmful or inappropriate content online – e.g. the IWF for illegal material, the site host for inappropriate material, their filtering product provider where they identify over- or under-blocking.

- Increased awareness among parents and children of the role that they can play, both in labelling the content they put online and in 'community policing'.

- Alignment of the advice and information that is being given to parents, teachers and children.

    - Integrated awareness-raising and educational initiatives, targeted at parents, teachers and children, at a local and national level, for maximum effect.

    - Linked to this, the broader inclusion of e-safety, along with the other critical components of media literacy, across the national curriculum from a younger age.

Delivering these outcomes

A very broad range of good initiatives are currently under way in this area – from those associated with formal government agencies such as Becta or the Child Exploitation and Online Protection centre (CEOP), to those offered by charitable organisations, industry bodies and individual industry players, including organisations such as Childnet International, Media Smart, the BFI, the Media Literacy Task Force , the BBC and Channel

[6] See below, 'The promotion of industry self-regulation' and Chapter 6 for more on this.

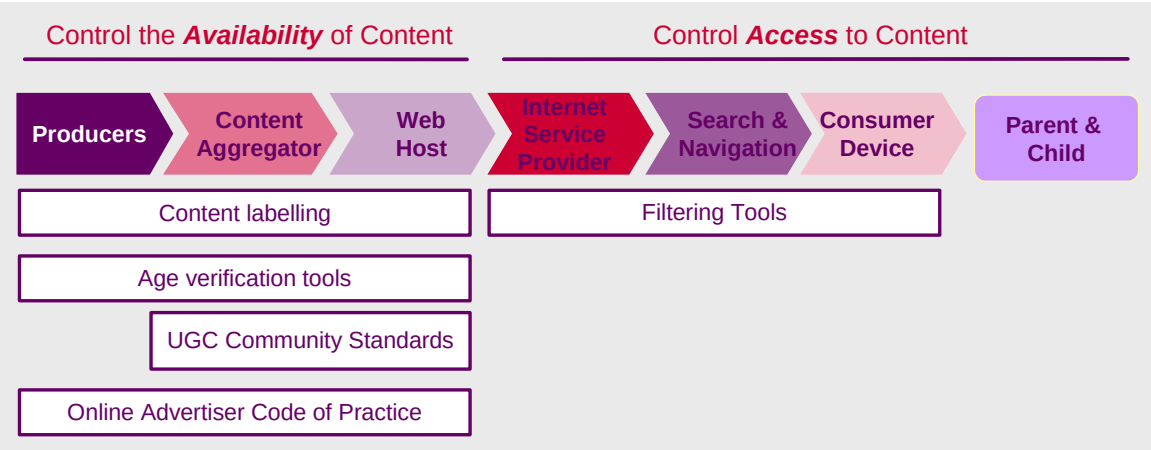
4[7]. However, to deliver the outcomes offered for consideration above, we propose that thought is also given to the following:

- The development of a framing strategy for the delivery of the above outcomes across the various government departments, industry bodies and individual industry players, charitable organisations, and regulators, with a single point of oversight and coordination.
    - Development of short-, medium- and long-term targets and the identification of the communications plan, educational initiatives and funding necessary to deliver these on a sustainable basis.
        - Consider the appropriate balance between a high level public information/awareness campaign and on-the-ground activities.
        - Prioritise the more vulnerable children.
    - Creation of communications and materials that are target-group specific, i.e. tailored to the different types of parents, children and teachers, so that they are appropriate to the level of the recipients' skills and understanding.
- The development and promotion of an easy-to-use and interactive online 'one-stop-shop' for information on how to protect children online, to help parents, children and teachers.

We have outlined our thoughts on the desired ends and described some of the possible means, but there is still the question for the Review team to consider about what is the institutional mix to make this happen (i.e. what is the role for Government, Ofcom, the BBC, schools, CEOP, industry etc.), as well as the appropriate funding model.

The promotion of industry self-regulation

Ofcom's suggestions to the Byron Review on Media Literacy are of crucial importance. In addition, there are five areas where we believe there may be an opportunity for further industry-led initiatives to support parents and children in their management of potentially harmful content. Ofcom suggests to the Review team that they give consideration to these areas for potential action**. Our suggestions involve, for the most part, a refocusing or widening of activity that is already under way in the marketplace: we are not proposing new regulatory interventions; rather, we are taking those that the market and/or Ofcom has already recognised and promoting the best of them.**



[7] See Annex 2 for more details

Ofcom's analysis employs a value-chain model of the internet content market[8]: we consider what different contributions industry players at each stage of the value chain can make. In the self-regulatory context we have described, these industry contributions are typically aimed at empowering or enabling parents and children to manage their content experience, and in particular to avoid potentially harmful content.

The five areas which we suggest the Byron Team considers are, in broad order of importance: filtering, content labelling, User Generated Content (UGC) community standards, online advertiser codes of practice, and age verification. For the most part, these are areas in which there is already significant voluntary industry activity under way.

The use of **filtering tools** is an essential element in the management of content risks; they have already been adopted by over half the UK's parents. In relation to filtering, we consider there are four further ideas worth exploring:

1. We recommend that the Byron team considers exploring with ISPs and the Internet Service Providers Association,(ISPA) their trade association, the development of a code of practice for family-friendly internet access, with relevant characteristics including the provisions of tools, information and support – for example in relation to parental controls for content filtering, and internet security (firewalls, spam-blocking tools). This code might also create a 'trustmark' or brand for family-friendly services, like those developed in France and Australia by ISPs and service providers. Information and awareness initiatives could improve parental awareness of the potential benefits of such services and of the trustmark. This could help to create incentives for interested ISPs to focus greater attention on creating differentiated family-friendly access propositions.

2. In the UK, Ofcom has been working with the Home Office and industry to develop a BSI standard for filtering products, which will allow qualifying products to carry a Kitemark. Alongside other media literacy initiatives, we recommend that the Byron team considers promoting awareness of Kitemarked filtering products' benefits, and encouraging their wider adoption.

3. As well as promoting the use of filtering products, we recommend that the Byron team considers ways of encouraging parents to be active users of such products, reporting instances of under- and over-blocking to their software providers. Over time, this information will help the development of products which better reflect the specific concerns and content standards of UK parents.

4. We recommend that the Byron Review considers encouraging the mobile network operators to extend their commitment to network filtering, and allowing parents to specify a child-friendly filtering option analogous to that possible within most PC filtering tools (e.g. an age 12+ filter in addition to the 18+ one that is currently in place).

Content information is also an essential element in the management of content risks; we recommend the Byron Review team considers promoting and supporting the efforts described below to improve the quality of content information in relation to commercially produced audiovisual media:

5. The Broadband Stakeholder Group, supported by Ofcom and key industry players, is developing common principles for the ways in which viewers should be informed about potentially harmful or offensive commercially produced audiovisual content. These

[8] Annex 1 includes a description of the value chain activities; Annex 2 describes the current activity in content protection at each stage of the value chain

common principles, once agreed by industry, will form the basis of good practice in enabling viewers to protect themselves and their children from exposure to such content.

6. Looking forward, the new Audiovisual Media Services Directive requires the UK to create a new regulatory framework for on-demand television service providers, including those operating on the internet. The UK is in the early stages of developing this model; however, effective and consistently applied content information is likely to be a significant element of the framework, along with other measures to control children's access to harmful content familiar from broadcast markets, such as PIN controls.

User-generated content (UGC) community standards are the frameworks and processes through which UGC hosts, like YouTube or MySpace, define the types of content they will host and determine how they will deal with complaints. As outlined above, we believe that individuals should be encouraged to participate in the 'community policing' of the sites they use, where such tools exist. While the tools for community content management are often sophisticated, their operation is often opaque to the audience, and their effectiveness has been questioned.

7. We recommend the Byron Review team consider working with industry to create a voluntary scheme or code under which UGC providers make transparent the operation of their content review processes – for example, reporting on the turnaround times for these processes, on the timetable (if any) for communicating with complainants, and ideally, with independent verification of performance. This type of scheme could mirror the commitment made by Facebook to the New York Attorney General concerning its complaints-handling process, under which Facebook sets targets and makes reporting commitments in relation to complaints about sexually explicit content.

We recommend the Byron Review team considers exploring with the **online advertising industry** ways to reduce further the extent to which mainstream UK online advertising is placed around harmful content. Initiatives might include:

8. Encouraging greater take-up of the IASH[9] Code (or a similar framework) so that it covers a much greater proportion of UK online advertising sales; and

9. Information/educational initiatives directed at improving awareness among advertisers and agencies of the means through which online advertising can be made more secure.

Finally, although **age verification** has the potential to be valuable in managing risks to children, practical hurdles, including implementation and cost, will tend to limit its impact. Nonetheless, Ofcom recommend that the Byron Review team considers whether there might be any opportunity to encourage the use of age verification to restrict access to harmful content.

[9] IASH = Independent Advertising Sales House

Conclusion

It is our view that, taken together, the combination of enhanced media literacy skills on the part of parents, children and young people, and targeted industry, NGO, regulatory and government initiatives, will help deliver an environment in which:

- parents are more confident of their ability to support their children online; and
- children themselves are confident in their online e-safety and also know what to do when they come across material that is potentially harmful or offensive.

We would encourage the Byron Review team to consider what success would look like. This could frame an independent further review within two years of implementation of the recommendations, asking:

- Whether there is any further evidence regarding harm and the level of risk which should be taken into consideration;
- Whether satisfactory progress has been made in relation to the concerns raised and if not, whether alternative measures need to be pursued.

Section 3

The benefits of the internet

This chapter briefly outlines the benefits and opportunities that the internet offers for children and young people. The key findings are as follows:

The vast majority of parents agreed that online, children discover interesting and useful things that they did not know before, and both parents and children overwhelmingly agreed that the internet helps children with schoolwork/ college.

Although the research is not conclusive, an analysis of the evidence does highlight the many apparent benefits of the internet and the opportunities it affords for social and educational achievement.

While TV remains the dominant medium for children aged 5-15, the importance of the internet to the child increases with age in its status as the medium the child would miss the most.

Most parents and children interviewed agreed that children who do not have/use the internet are at a disadvantage.

While not an issue directly raised by the Byron Review team, the evidence also highlights the inequalities that exist regarding children's access to the internet and the potential adverse implications of this for those children.

The internet is a powerful platform for the distribution of services to audiences. It is a network of networks, spanning the world, and connecting a global audience with a globally provided set of content and services: almost any member of society from almost anywhere in the world can gain access to content and services produced by anyone and hosted anywhere on the global network. The simplicity of the protocols on which the internet is based, and the flexibility of the devices through which most audiences connect to the internet, enable an extraordinary range of services to be created and used. Together these factors – global reach and flexibility – have made the internet an engine for innovation throughout our society: in media, communications, and business.

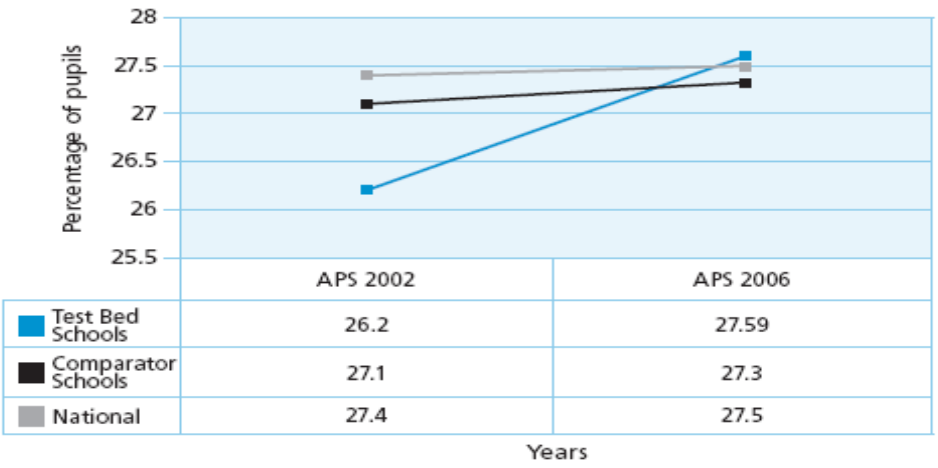
In the market research conducted for this submission[10], the vast majority of parents agreed that online children discover interesting, useful things that they did not know before (92% of parents). Parents, young people and children[11] all overwhelmingly agreed[12] that the internet helps children with school/college work (92% of parents and 81% of children).

In Becta's *Harnessing Technology Review 2007: Progress and impact of technology in education*, it is noted that:

[10] See Annex 5, for the full research report
[11] Children and young people aged 8-17, n = 513.
[12] Agree strongly or agree slightly, i.e. top 2 box score. Top 2 box – or bottom 2 box – scores are cited unless otherwise staged

"There is increasing evidence that the use of ICT can help raise educational standards, though this is influenced by the context in which the technology is used. Links between e-maturity and school performance have been demonstrated both through analysis of national data and the evaluation of the ICT Test Bed project. The latter found a strong improvement in the attainment of pupils (see figure 1), particularly at Key Stage 2."

Figure 1 Comparison of Test Bed schools with the national picture and comparator schools in core subjects



	APS 2002	APS 2006
Test Bed Schools	26.2	27.59
Comparator Schools	27.1	27.3
National	27.4	27.5

Source: Evaluation of the ICT Test Bed Project Final Report (2007) (Somekh, Underwood et al., 2007)

The report also goes on to say that: "Where technology is used to support learning, even if utilised purely to enhance existing practice, we can now be confident there is a positive general impact on learning outcomes. Since the 2003 ImpaCT2 study, statistical links between the use of technology and learning outcomes have been identified in an increasing body of evidence, ranging from studies of home use of ICT by learners, to studies of the impact of specific technologies (for example, interactive whiteboards) on learning, and analysis of the relationship between the development of school e-maturity and school improvement. In the FE and skills sector, robust evidence of impact on outcomes is limited."

Research with primary and secondary school teachers, published in this report, also points to the positive motivational and attainment impact of ICT on pupils:

Table 1: Primary teachers' views of impact of ICT (percentage agreeing ICT can have a positive impact on the groups listed)

	Motivation		Attainment		Base (all primary teachers answering)
	Agree Strongly %	Agree %	Agree Strongly %	Agree %	
Key Stage 1 pupils	49	45	26	48	539/535
Key Stage 2 pupils	56	42	27	52	559/552
Girls	43	53	24	53	594/580
Boys	59	39	29	50	595/580
Able or gifted & talented pupils	53	42	29	49	598/586
Pupils with special educational needs	58	39	32	51	600/586

Source: Harnessing Technology in Schools survey 2006 (Kitchen, Finch and Sinclair, 2007)

Table 2: Secondary teachers' views of impact of ICT (percentage agreeing ICT can have a positive impact on the groups listed)

	Motivation		Attainment		Base (all primary teachers answering)
	Agree Strongly %	Agree %	Agree Strongly %	Agree %	
Key Stage 3 pupils	42	49	20	47	1184/1174
Key Stage 4 pupils	38	51	23	47	1162/1150
Girls	30	52	19	47	1167/1156
Boys	47	45	23	48	1153/1143
Able or gifted & talented pupils	39	47	23	45	1179/1173
Pupils with special educational needs	45	46	26	47	1173/1163

Source: Harnessing Technology in Schools survey 2006 (Kitchen, Finch and Sinclair, 2007)

Around two-thirds of the parents (67% of parents of 8-17 year olds) and children (64% of 8-17 year olds) interviewed in research conducted for this submission agreed that children who do not have/use the internet are at a disadvantage. Agreement with this statement increases with the age of the child in the household – 58% of parents of 5-7 year olds agree, rising to 69% of parents of 16-17 year olds. Around one in four parents and one in five children aged 8-17 disagreed with this statement – in other words did not agree that children who do not have/use the internet are at a disadvantage; those who have/ are children who access the internet but not from home are more likely to disagree (43% and 30% respectively), as are C2 children and DE parents (35% and 34% respectively).

The findings about internet access being an advantage to children are consistent with a qualitative study conducted earlier on this year by Ofcom's Consumer Panel: in *Children and the Internet*[13] it is reported that from about age ten, most children believe that internet access is a 'must have'. Key benefits for children were found to centre on social communication and inclusion – the internet enabled those children who were not in the 'in crowd' to participate, as their personalities could shine through in the more impersonal communication over the internet. Educational achievement was of secondary importance to

[13] Ofcom Consumer Panel 2007. http://www.ofcomconsumerpanel.org.uk/information/documents/Children_and_the_internet.pdf

many of the children; however, from the age of 10 onwards, there was a reported pressure from schools for families to get the internet and a sense that access to the internet allowed willing students to attain a higher quality of presentation and content. The research also suggested that use of the internet had a role in re-engaging some of the educationally disengaged, as they enjoyed the control and fun of working with a PC. Children who didn't have home internet access believed that they had inferior technical skills to those who did. The report also found that children who were already on the outside of their social peer group risked becoming further isolated without internet access. However, the study found that having the internet at home did not guarantee social and educational achievement. It strongly depended on how the internet was used and controlled and the type of child who was using it.

From a labour-market perspective, awareness and the ability to use ICT is recognised increasingly as a basic skills requirement, and the Skills Strategy recognises ICT as the third essential 'Skill for Life' (alongside literacy and numeracy)[14]. The internet enables learning to occur not only in educational institutions, but also at home, and to be personalised to a greater degree – although not all the research found beneficial effects and there is debate about the effect of other variables and timescales. What does seem to be critical is the way in which ICT is used and some commentators argue that there has been a lack of training for teachers in this area.

As noted in a recent report by Futurelab: "Whilst ICT use is certainly not a pre-requisite to surviving in 21st century society…, it is almost certainly an integral element of thriving in 21st century society."[15]

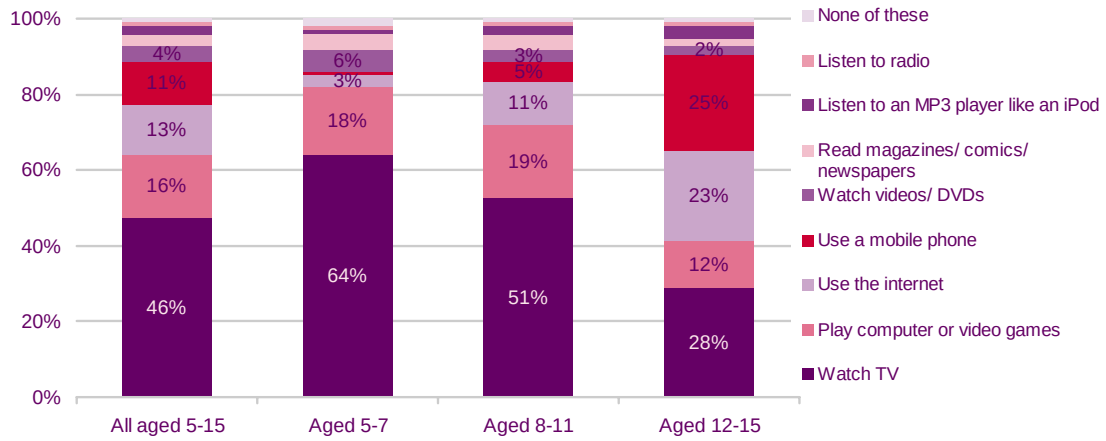
While the majority of children access the internet at school, and recent figures show that 64% of children aged 5 to 15 use the internet at home, home internet access is not consistent across social and economic groups: 81% of children from AB families access the internet at home, compared to 46% of children from DE families[16].

The IPPR[17] notes that lack of engagement with ICT cannot be explained simply in terms of access and skills. "It is becoming increasingly clear that it is a social, economic and *cultural* phenomenon, relating to motivation, confidence, assistance and the type of content available on the internet." The IPPR suggests that the digital divide is a symptom of economic inequality, and not a cause, and so: "exclusion from technological networks tends to go hand in hand with a variety of other forms of exclusion. These include: low skills; lack of confidence in ICT use and general literacy; lack of informal technical support (i.e. friends and family with good skills); and lack of social reasons to use ICT (e.g. if one's peers are not using email, for instance, then that removes much of the incentive to use it)".

The increasingly important role of the internet, particularly for older children, is further demonstrated when we ask them what media activity they would miss the most. As can be seen in Figure 2 below, the importance of TV declines with age while that of the internet - and mobile phones - increases. This is a trend that appears to be accelerating. For example, Ofcom's 2005 research into media literacy found that 6% of 8-11 year olds and 8% of 12-15 year olds said they would miss the internet the most, compared to 11% of 8-11 year olds and 23% of 12-15 year olds in 2007.

[14] The impact of government policy on social exclusion among working age people: A review of the literature for the Social Exclusion Unit in the Breaking the Cycle series (August 2004)
[15] Futurelab: Beyond the Digital Divide Rethinking digital inclusion for the 21st century (2007)
[16] Young People and Media Survey – Ofcom 2007
[17] IPPR – Modernising with Purpose: A Manifesto for a Digital Britain

Figure 2 Media activity children would miss most



Q: Now of the ones you do almost every day, which one of these would you miss doing the most if it got taken away?
Base: Children aged 5-15 (3,696)
Source: Ofcom – Young People & Media, April - September 2007

Section 4

Children's safety and wellbeing when online

This chapter summarises the findings from a range of consumer research studies looking at: children's use of the internet; rules around use of the internet in the home and ways in which parents are currently trying to make the internet a safe experience for their children; attitudes to the internet – both benefits and concerns; current level of exposure to potentially harmful or inappropriate material online, and the actions taken when exposed.[18]

Where possible the research looks at the viewpoint and experiences of both parents and children in order to understand gaps and differences in knowledge, perceptions and attitudes.

The key findings are as follows:

The internet is much used and valued by children, young people and parents, and the importance of the internet to the child increases with age.

- Overall, 99% of children aged 8-17 say that they use the internet, and 80% of households with children aged 5-17 have internet access at home (compared to 57% of households without children).
- While TV remains the dominant medium for children aged 5-15, the use and importance of the internet to the child increases with age, both in terms of hours of use and in its status as the medium the child would miss the most.
- Average hours of use of the internet have increased greatly over the past two years (from 7.1 hours/week in 2005 to 13.8 hours/week in 2007 for 12-15 year-olds).
- The uses made of the internet by children vary considerably by age: younger children tend to use it more to play games, older children as an educational tool as well as for searching, email, watching or downloading video clips, and using social networking sites.

A mixed picture emerges regarding the degree and effectiveness of parental oversight of internet use at home.

- For a start, one of the challenges faced by parents is that almost half (47%), believe their child is more skilled at using the internet than they are. This is especially true of the parents of older children (61% of parents of 12-17 year olds).
- There are also differences in what parents and young people say about the presence of 'internet rules' at home: the research indicates that parents tend to claim greater presence and use of these rules compared to children, especially in the case of children under 15.
- Just over half of parents said that they had content filtering software installed; a further 9% said that they had not heard of filtering (until now) but would be interested in using it in the future. Around one in five was familiar with content

[18] See Annex 5 for the full research report and methodological overview. Most of the findings referred to in this chapter are drawn from the research conducted for this review (Children, Young People and Online Content) or Ofcom's Young People and Media tracking study (April – September 2007).

filtering software, but did not use it, mainly because they trusted their children. This suggests that parents think that this type of software is used to prevent children from accessing certain types of content rather than as a tool which could be used to help provide protection from such material. Other reasons mentioned were that their children were too young to surf the web, or because they did not think they needed it.

- While parents generally seem to have a good understanding of what their child uses the internet for at home, there are some notable exceptions: they seem to be underestimating, in particular: game playing, watching video clips, using social networking sites and contributing comments to someone else's web page. This is borne out, for example, by the finding that around one in five parents do not know if their child has a social networking site profile.
    - One possible reason for this is unsupervised use; overall, 16% of children have a computer with internet access in their bedroom (this rises from 1% of 5-7 year olds, to 12% of 8-11 year olds and 24% of12-17 year olds); parents also tend to underestimate their child's access to the internet at a friends house.
- Finally, while the majority of parents believe that they have done what needs to be done to help their child stay safe when online, there is a sizeable group of parents (over one in four) who say that they do not have any rules in place.
- This points to, on the one hand, a group of parents who may not be doing enough to ensure that their children are safe online, and, on the other hand, to another group who have rules in place, but where there are potential shortfalls in the effectiveness of these rules.

While almost one in seven children[19] say they have come across potentially harmful or inappropriate material in the past six months, almost one in ten parents[20] do not know if they have or not. The likelihood of coming across such material increases with the age of the child, as does the likelihood of the parent not knowing if the child/young person has.

- While the majority of children and parents agree that the child would tell the parent if they came across something that worried them, this does not always seem to be the case: overall, 16% of 8-17 year olds say they have come across harmful or inappropriate material[21] in the past six months, while 12% of parents with children in this age group say that their child has; almost one in ten parents (8%) do not know if their child has come across harmful or inappropriate content in the past six months.
- Responses from parents and children indicate that most of this material was seen at home, but children also say that they have seen it at school or at friends'/relatives' houses. Parents seem to be less aware of out-of-home exposure to potentially harmful or inappropriate content. This clearly has implications for the impact of their rules on the child's levels of potential exposure and risk.
- Sexual content is by far the most frequently mentioned type of inappropriate content, followed by violence and pop-up adverts with harmful or inappropriate content.
- Most children say that they leave the site when they come across such material, with only a small percentage saying that they tell a parent (possibly because they are not sufficiently concerned or worried about it).

[19] Children aged 8-17
[20] Parents of children aged 8-17
[21] We asked first of all if they had come across harmful or inappropriate material in the past 6 months and if they had, we asked the open-ended question 'What type of content was it?'. Thus these findings relate to self-reported harmful or inappropriate material.

The majority of parents (57%) do not know where to go to get information about how to help protect their children online.

- Between 5%-8% mentioned other websites, family/friends, or the library; 3% or less mentioned *Get Safe Online*, *ThinkYouKnow,* the Internet Watch Foundation or CEOP (Child Exploitation and Online Protection).

A substantial minority of parents – almost four in ten – would not know who to complain to if they came across something potentially harmful or inappropriate.

- Around a third would complain to the police, 14% to their ISP and 11% to the websites themselves. Most children say they would complain to their parents (though whether they would or not is questionable, given the findings reported above).

Although parents and children do have concerns about the internet, for both, the benefits outweigh the risks.

- In research conducted for this submission, the vast majority of parents agreed that online children discover interesting, useful things that they did not know before, and both parents and children overwhelmingly agreed that the internet helps children with school/college work.
- Almost two-thirds of the parents and children interviewed in this research agreed that children who do not have/use the internet are at a disadvantage.
- The majority of parents agreed that they trusted their child to use the internet safely, and that it was safe for them to go online and in general the children interviewed were more confident of their ability to manage online risk than their parents were.
- While the majority of parents clearly have concerns about the internet (66% of all parents have concerns), the reverse is true of children (30% of 8-17 year olds have concerns). Parents have concerns about risks on the internet (especially regarding sexual content, paedophiles masquerading as children, child abuse imagery and bad language).
- While parents overwhelmingly believe that internet users must be protected from seeing inappropriate or offensive content, slightly more than half agree that internet sites must be free to be expressive and creative.
- Finally, a majority of parents think that the benefits of the internet outweigh the risks, and that real-life concerns like bullying and violence are more worrying. Children in particular agree with the latter statement.

4.1 Media use in the home

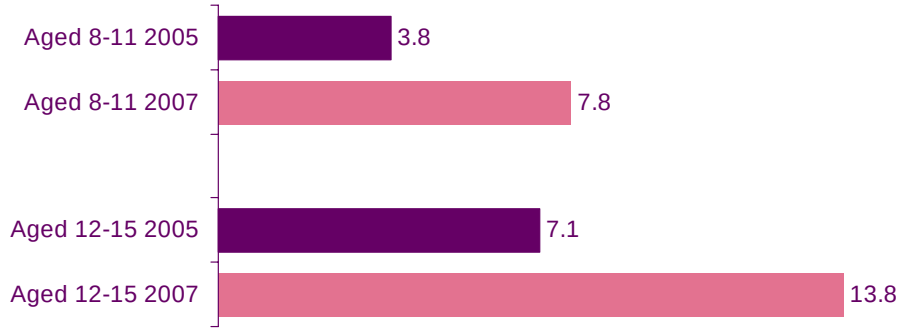
Overall, 80% of households with children aged 5-17 have computers with internet access in the home, compared to 57% of households where children are not present.

Ownership of media-related technologies in general tends to be higher in households with children, and in particular in households with older children, than in those without.

Children's bedrooms are increasingly becoming multi-media centres: for example, 48% of children aged 5-17 have analogue TV in their bedroom, 24% have multichannel television, 55% a games console, 16% a PC with internet access, 9% a webcam, while 61% own a mobile phone. In general, these figures are even higher for older children (e.g. around a quarter of 12-17 year olds have a computer with internet access in their bedroom).

While TV remains the dominant medium for children the average number of hours spent online increases considerably for older children. The average number of hours spent online has also increased greatly over the past two years:

Figure 3 Hours use the internet at home in a typical week (Child responses) – 2005 vs. 2007



Q: 2005 – How many hours would you say you spend using the internet at home in a typical week? 2007-Thinking about the time you spend using the Internet at home. How many hours would you say you use the internet on a typical school day/ weekend day?
Base: All who use the internet at home: Children aged 8-11 (2005= 378, 2007=877), 12-15 (2005 = 467, 2007=1040)
Source: Ofcom – Media Literacy Audit 2005/ Young People & Media, April - September 2007

These findings are consistent with those reported in Chapter 3: the importance of the internet to the child increases with age (older children are more likely than younger ones to say that the internet is the medium that they would miss the most).

4.2 Location of children's internet access

Overall, 99% of the 8-17 year old children interviewed say that they use the internet, the majority either at home and/or at school; almost one in five have access to the internet only outside their home.

Table 3 Children's access to the internet - Summary

	Any access : 8-17 year olds	Most often access: 8-17 year olds
PC/laptop at home	81%	65%
School/college	86%	26%
Library	12%	1%
Internet cafe	3%	
Friend's house	23%	2%
Relative's house	11%	2%
Mobile phone	7%	1%
Any internet use	99%	
Don't use the internet	1%	
Use internet but not at home	18%	

Q. Do you use the internet nowadays? If so, where do you access it? Where do you access it most often?
Base: Children 8-17 (513)
Source: Ofcom – Children, Young People & Online Content, October 2007

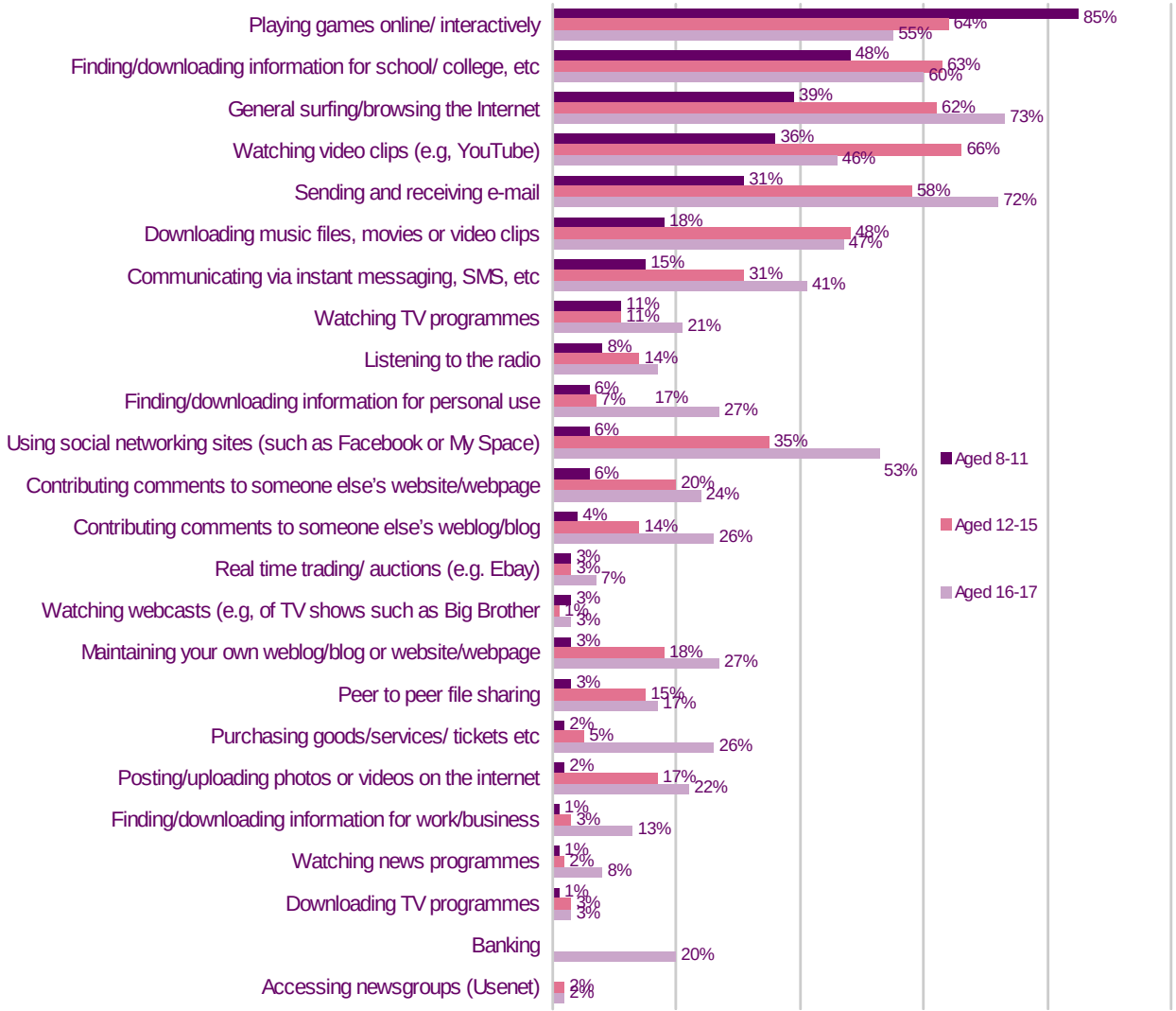
Parents' and children's responses to the question of where children access the internet are consistent for most locations, with one exception: parents underestimate access to the internet at a friend's house. Only 10% of parents of 8-17 year olds say that their child accesses the internet there, compared to 23% of children aged 8-17.

Responses from parents and children regarding the child's use of his/her mobile to access the internet are broadly consistent; according to the children interviewed, mobile phones are used by 7% of 8-17 year olds to access the internet – this is driven by the older age groups, specifically the 16-17 year olds (14% access the internet via a mobile phone).

4.3 Children's use of the internet in the home

The uses made of the internet by children vary quite considerably by age: younger children tend to use it more to play games, older children as an educational tool as well as for searching, email, watching or downloading video clips, and using social networking sites:

Figure 4 Children's use of the internet by age group



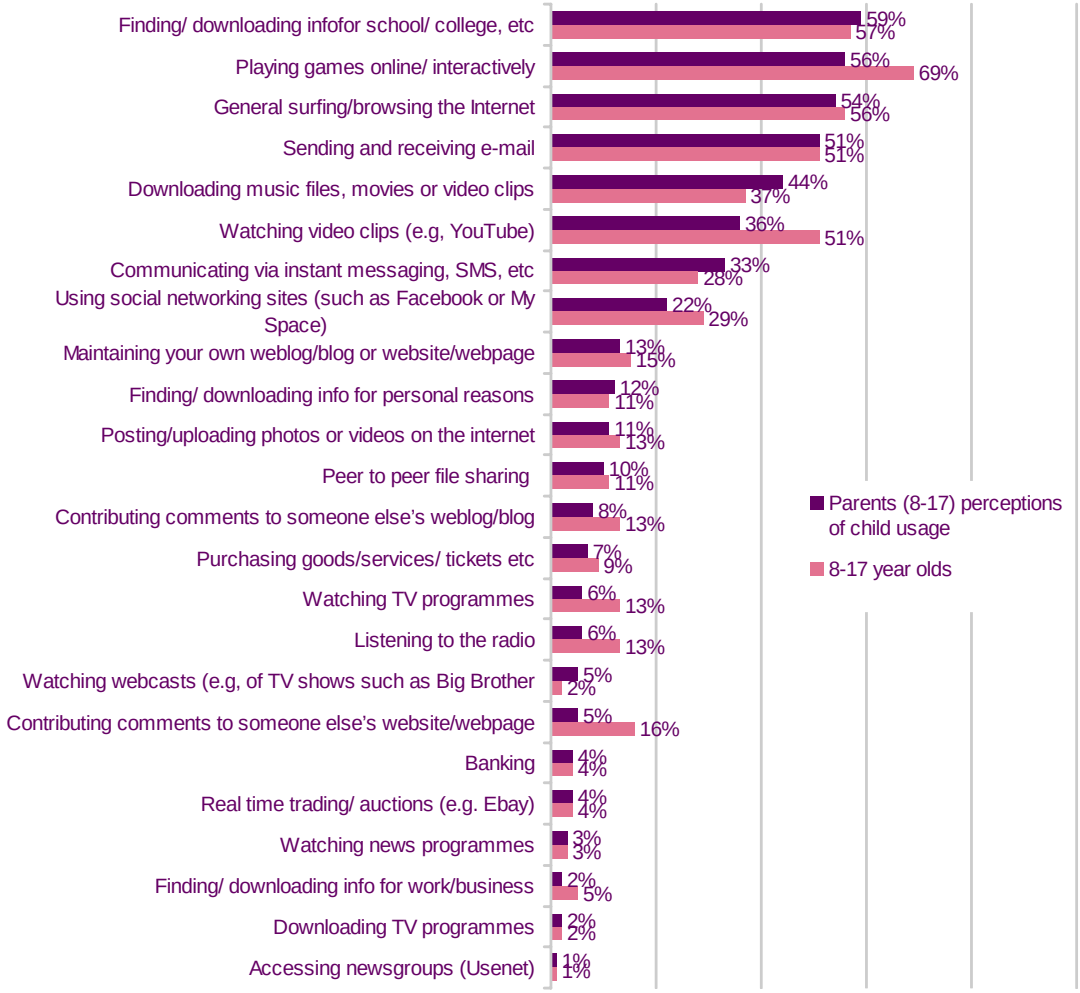
Q: Which, if any, of these do you use the Internet for?
Base: All who use the internet at home: Children aged 8-11 (147), 12-15 (188), 16-17 (89)
Source: Ofcom – Children, Young People & Online Content, October 2007

Results from Ofcom's tracking study: *Young People & Media* finds that the majority of 5-7 year olds (69%) are supervised by an adult when using the internet at home. This falls to 28% of 12-15 year olds, who are more likely to be accessing the internet on their own (63%). This may be linked to the trend for increased penetration of computers with internet access in older children's bedrooms.

When we compare the responses of parents and children we see that, for the most part, parents have good understanding of how much time their child is spending online and what their child uses the internet for at home. However, there are some notable exceptions:

parents seem to be underestimating, in particular, game-playing, watching video clips, using social networking sites and contributing comments to someone else's website/webpage:

Figure 5 Children's use of the internet at home: Parents' perceptions vs. children's responses



Q: Which, if any, of these do you use the Internet for? Which, if any, does your child use the internet for?
Base: All whose child/who use the internet at home: Parents of 8-17 year olds (445), 8-17 year olds (424)
Source: Ofcom – Children, Young People & Online Content, October 2007

4.4 Parents' and children's internet skills

While 47% of parents think that the child/children in the house are more skilled than they/their partner are, there are considerable variations by age: parents of younger children are more likely to think that they - the parents - are more skilled than their child and vice versa for parents of older children:

- 72% of parents of children aged 5-7 say that they (or the other parent) are more skilled,
- 61% of parents of 12-17 year olds say that their child is the more skilled.

This assessment is consistent with children's views on who is the more skilled, themselves or their parents.

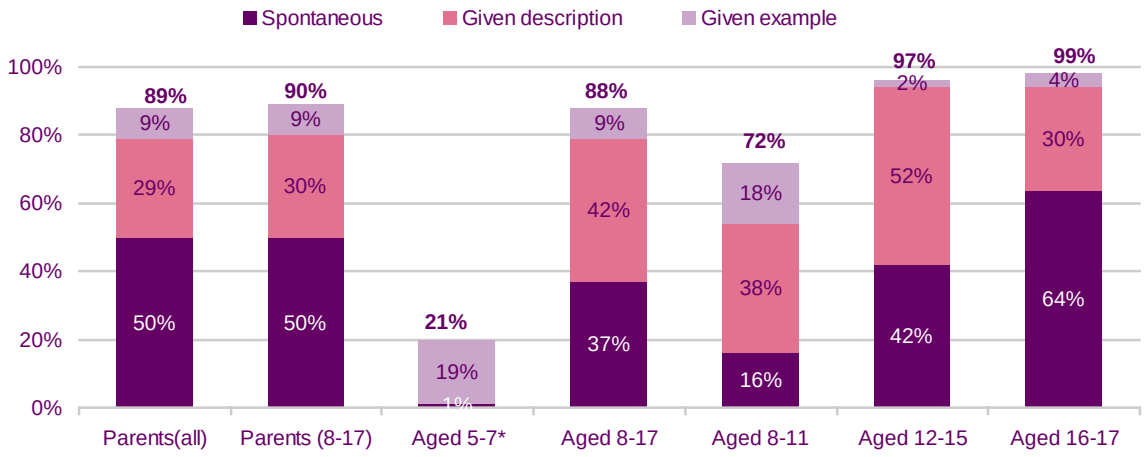
4.5 Children's and parents' awareness and use of social networking and user-generated content sites

As reported above, two popular uses of the internet among children, and particularly older children, are visiting social networking sites and watching video clips on user-generated content sites, and parents tended to underestimate this usage. This section looks in brief at the differences between parents and their children with regard to social networking and user-generated content sites.

Children's and parents' awareness and use of social networking sites

Half of the parents interviewed had heard of the terms 'social networking sites' (SNS) and a further third had head of them after being given their description. 16-17 year olds have the highest levels of spontaneous awareness of SNS, and this was lowest amongst 5-7 year olds:

Figure 6 Awareness of SNS - Parents vs. children



Q: Are you familiar with the term 'Social Networking Sites'?
**5-7: given description and example in the same question*
Base: Parents of 5-17 year olds (653), parents of 8-17 year olds (537), children aged 5-7 (140), 8-11 (198), 12-15 (208), 16-17 (107)
Source: Ofcom – Children, Young People & Online Content, October 2007

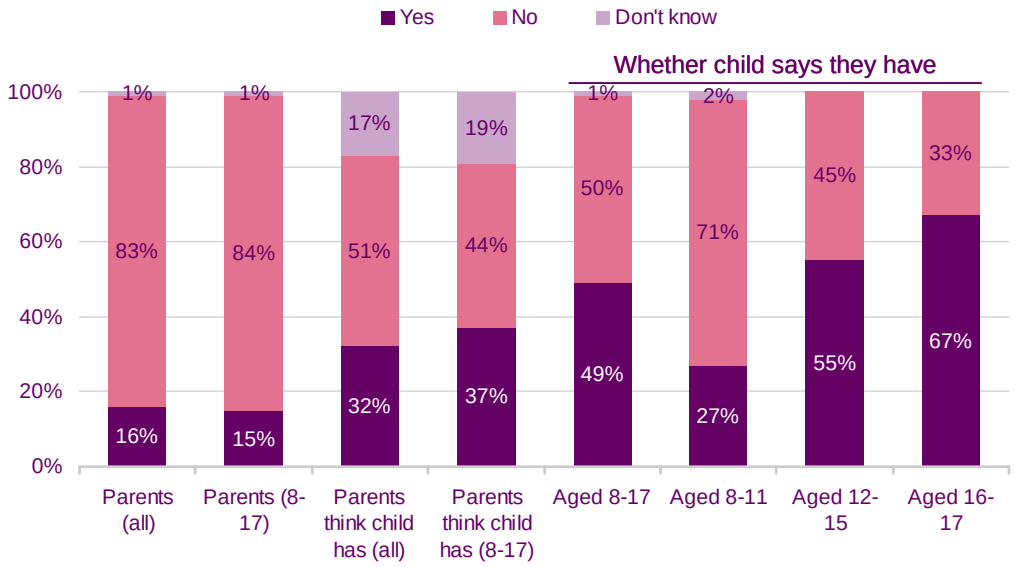
Older children are far more likely to have an SNS profile than younger children, and children in general are far more likely to have a profile than are parents:

- 16% of all parents aware of social networking sites say they have a profile on a site, compared to 27% of 8-11 year olds, 55% of 12-15 year olds and 67% of 16-17 year olds.

- This is equivalent to 15% of all parents having a profile, 19% of all 8-11 year olds, 54% of all 12-15 year olds and 66% of all 16-17 year olds.

While most parents are aware of these sites, many of them think that their child does not have a profile when in fact he/she says that they do, and almost one in five parents does not know if their child has a SNS profile:

Figure 7 Profiles on SNS – Parents vs. children



Q: Do you have a page or profile on a social network site? Does your child?
Base: All aware of social networking sites/whose child uses the internet –Parents of 5-17 year olds (579), parents of 8-17 year olds (481), children aged 8-17 (451), 8-11 (143), 12-15 (202), 16-17 (106)
Source: Ofcom – Children, Young People & Online Content, October 2007

More parents than children say that they have rules in place for SNS use (65% of parents of 8-17 year who believe that their child has a profile say that they have rules in place versus 53% of 8-17 year olds with a profile).

The key rules relate to

- restrictions on meeting new people online (30% of parents with 8-17 year olds, 13% of 8-17 year olds, the biggest gap)
- giving out personal details (27% of parents of 8-17 year olds, 26% of 8-17 year olds) and
- meeting online contacts in person (17% of parents of 8-17 year olds, 10% of 8-17 year olds).

Parents underestimate the extent of their children giving out personal information online, and almost one in ten do not know if their child does this:

- 23% of parents of 8-17 year olds say that their child has given out personal information online, compared to 36% of children aged 8-17.
- The biggest gaps are for those aged 12-15 (28% vs. 44%) and 16-17 (37% vs. 61%).

There is also a considerable gap between parents' awareness of the privacy setting of their child's SNS profile: When asked whether their child's profile was currently visible:

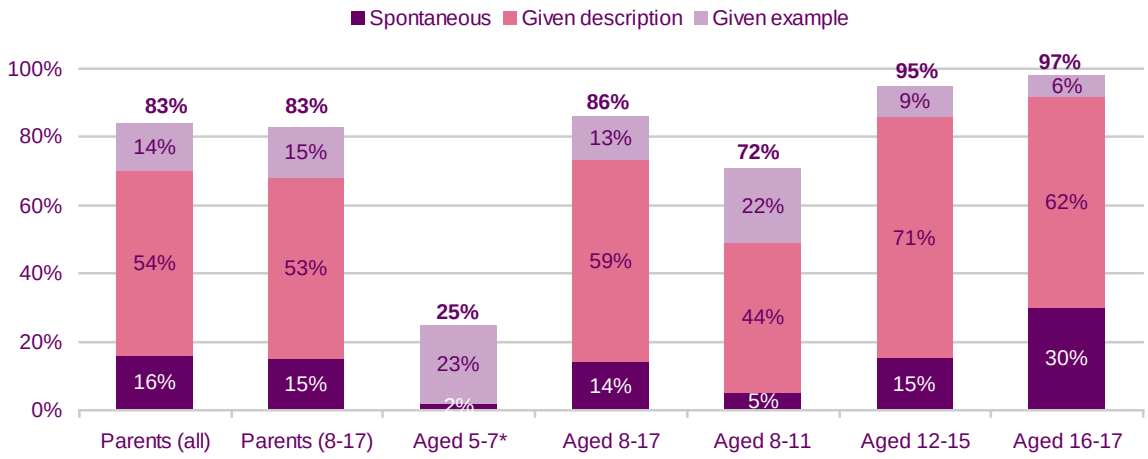
- 70% of parents of 8-17 year olds with a page on a social networking site said that it was, 10% said that is was not visible and 20% replied 'don't know'.
- This is in contrast to the 83% of 8-17 year olds with a profile who said their profile was currently visible.

However, of the parents who were aware that their child had a visible profile, most had a good understanding of its visibility to friends (53% of parents of 8-17 year olds said their child's profile was visible only to their friends, compared with 58% of 8-17 year old children).

Children's and parents' awareness and use of user-generated content sites

Spontaneous awareness of the term 'user-generated content sites' (UGC) is much lower than that recorded for social networking sites: just 15% of parents of 8-17 year olds and 14% of 8-17 year olds said they were aware of this term. However, awareness rose significantly after respondents were presented with a short description of these sites and further still when given examples of websites. Overall awareness is 83% among parents and 86% among 8-17 year olds.

Figure 8 Awareness of UGC sites – Parents vs. children

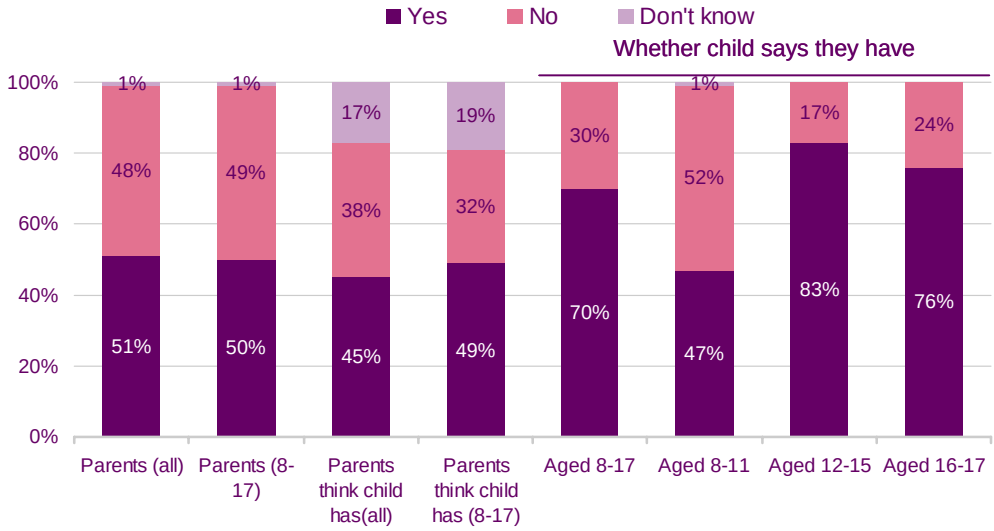


Q: Are you familiar with the term 'User Generated Content' sites?
Base: All parents (653), parents of children aged 8-17 (537), children aged 5-7 (140), 8-11 (198), 12-15 (208), 16-17 (107)
Source: Ofcom – Children, Young People & Online Content, October 2007

Older children and young people are more likely than younger children to have viewed content on UGC sites, and older children and young people in general are far more likely to have viewed content on these sites than their parents: 50% of parents of 8-17 year olds said that they had viewed content on a UGC site, compared to 47% of 8-11 year olds, 83% of 12-15 year olds and 76% of 16-17 year olds.

While most parents are aware of these sites, many of them think that their child has not viewed content on a UGC site when in fact the child says that he/she has (49% vs. 70%), and almost one in five parents do not know if their child has viewed any UGC in the past six months.

Figure 9 Viewed content on UGC sites – Parents vs. children



Q: Have you viewed any content (photos or videos) on a User Generated Content site, such as YouTube or Flickr in the last 6 months?
Base: All aware of user-generated content sites: Parents of children aged 5-17 (524), parents of children aged 8-17 (443), children aged 8-11 (142), 12-15 (197), 16-17 (104)
Source: Ofcom – Children, Young People & Online Content, October 2007

Compared with social networking sites, families are less likely to have rules in place around the use of UGC sites, but again, more parents than children say that there are rules in place: 46% of parents of children aged 8-17 said they had rules, somewhat higher than the 39% of 8-17 year olds who said this was the case.

Where rules exist, they are often either an all-out ban on visiting these sites, or restrictions relating to the viewing and posting of content (each is mentioned by around one in ten). Parents and children give similar accounts of the rules in place.

4.6 Rules about going online

While the majority of parents believe that they have done what needs to be done to help their child when online, almost one in ten do not believe they have done so…

- 84% of parents of 8-17 year olds agreed that they had provided their child with enough information to stay safe online, and 7% disagreed. The majority of children agreed with this (85% agreed, 6% disagreed).
    - This figure ranges from 86% of parents of 5-17 year olds whose child accesses the internet from home to 61% of those parents whose child uses the internet but does not have access at home
- 73% of parents with children aged 8-17 agreed that they had appropriate measures in place to keep children safe online; 8% disagreed.
    - This figure ranges from 79% of parents of 5-17 year olds whose child accesses the internet from home to 48% of those parents whose child uses the internet but does not have access at home

… and around a quarter say that they have not done any of the following:

- Discussed what they can or cannot do online (58% of parents of 8-17 year olds said they had done this; 54% of children aged 8-17 said that their parent had done this).
- Discussed how to stay safe online (overall, 56% of parents with children aged 8-17 said they had done this; 54% of children aged 8-17 said their parent had done this).
- Discussed, or shown their child how to search for information effectively (36% of parents said they had done this; 28% of children aged 8-17 said they had).
- Discussed, or shown their child how to decide if information online can be trusted or is reliable (31% of parents with 8-17 year olds said they had done this; 27% of children aged 8-17 said they had).

Overall, 80% of parents of 5-17 year olds whose child accesses the internet at home say they have done at least one of these; this falls to 45% of those parents whose child uses the internet but does not have access at home.

This points to, on the one hand, a group of parents who may not be doing enough to ensure that their children are safe online, and, on the other hand, to another group which has rules in place, but where there are potential shortfalls in the effectiveness of these rules.

While most parents and children say that there are rules/restrictions around the child's use of the internet, parents perceive a higher level of oversight in the home than their children do. The use of rules starts to fall off for children aged 12 and over in particular:

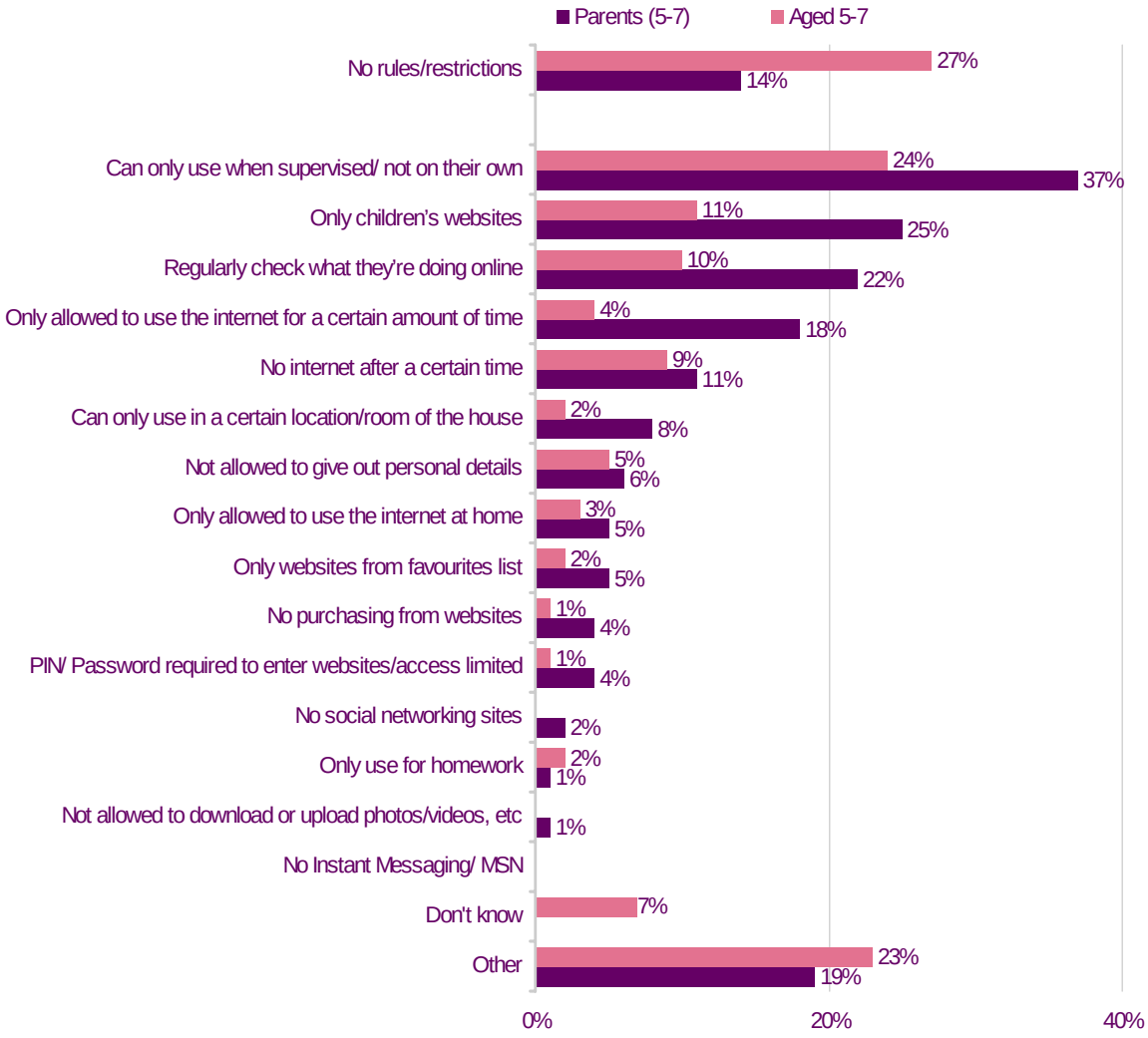
Table 4 Rules and restrictions around internet use: Summary

		5-7 year olds	8-17 year olds	8-11 year olds	12-15 year olds	16-17 year olds
Child responses						
Rules		66%	64%	71%	59%	59%
No rules		27%	36%	29%	41%	41%
Parent responses	**All**					
Rules	71%	86%	68%	81%	69%	50%
No rules	29%	14%	32%	19%	31%	50%

Q: Do you / your parents have any rules or restrictions about using the Internet?
Base: All who/whose children use(s) the internet: Parents of 5-17 year olds (621), parents of 8-17 year olds (526), children aged 5-7 (118), 8-11 (198), 12-15 (208), 16-17 (107)
5-7 year olds asked what rules rather than restrictions
Source: Ofcom – Children, Young People & Online Content, October 2007

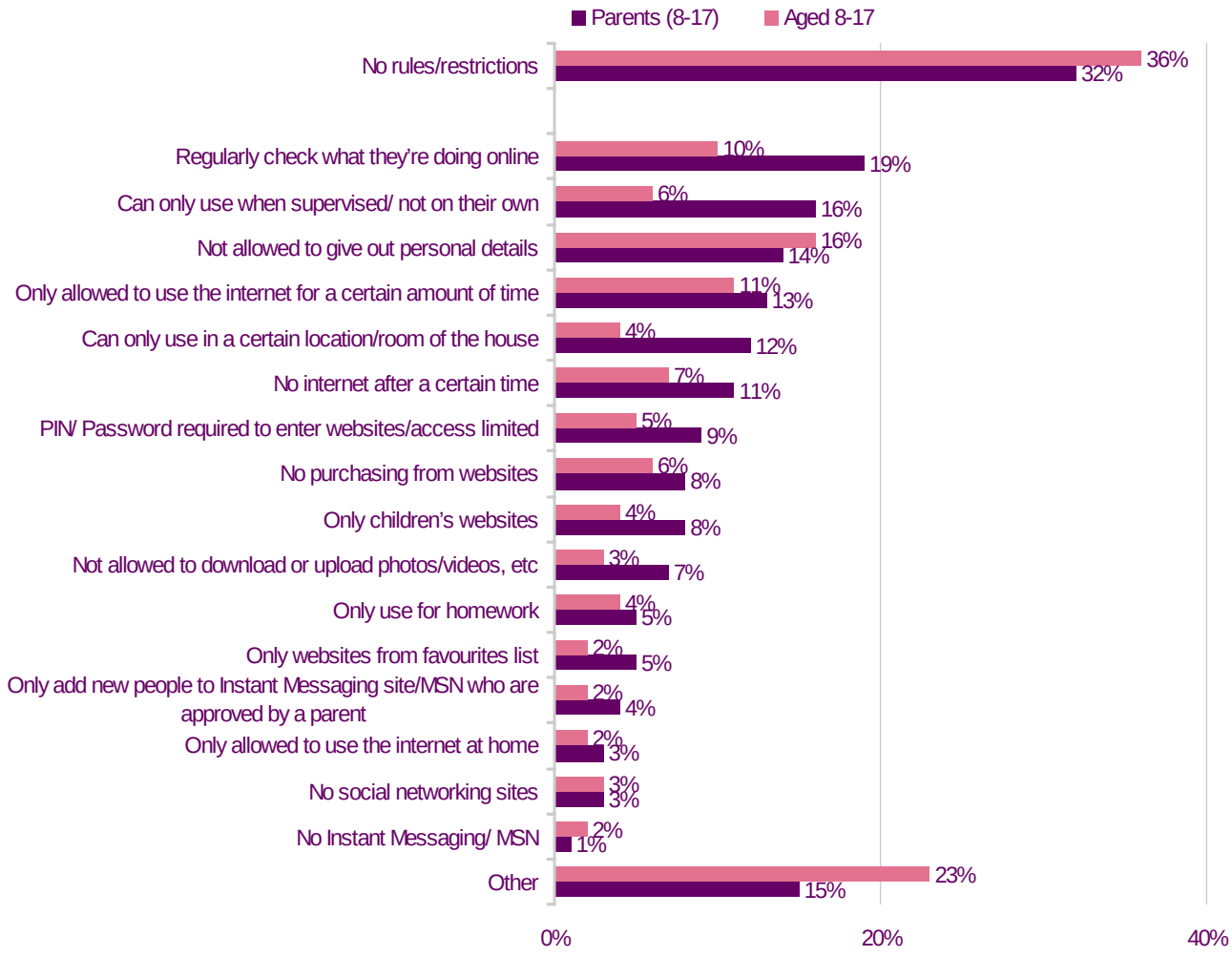
The following diagram summarises the rules implemented, by age of child, as reported by the parents and children. As can be seen, the most frequently mentioned rules relate to supervised use (although this is mentioned by around twice as may parents as children, which seems to undermine its credibility). Other rules relate to the protection of the child's privacy, the amount of time that can be spent online or the types of websites that can be accessed, etc. 9% of parents mention controlling their child's access with filters (see Section 4.7 for more on the use of content filtering software):

Figure 10 Presence of rules and restrictions relating to internet use: 5-7 year olds



Q: Do you / your parents have any rules or restrictions about using the Internet?
Base: All who/whose children use(s) the internet: Parents of 5-7 year olds (95), children aged 5-7 (118)
5-7 year olds asked what rules rather than restrictions
Source: Ofcom – Children, Young People & Online Content, October 2007

Figure 11 Presence of rules and restrictions relating to internet use: 8-17 year olds



Q: Do you / your parents have any rules or restrictions about using the Internet?
Base: All who/whose children use(s) the internet: Parents of 8-17 year olds (526), children aged 8-17 (513)
Source: Ofcom – Children, Young People & Online Content, October 2007

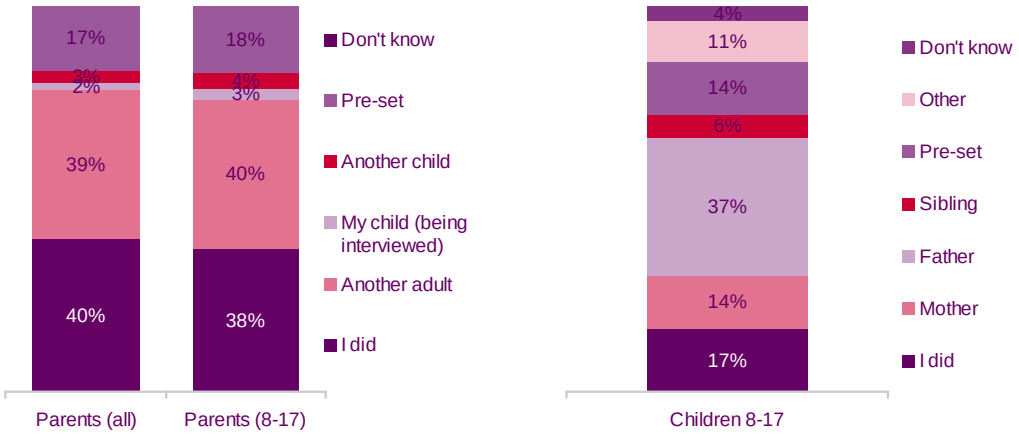
The majority of parents and children say that there are certain things that the child does not do online because they know it is dangerous (90% of parents of 8-17 year olds agreed and 86% of children aged 8-17).

4.7 Use of content filtering software

Overall, 83% of all parents are aware of content filtering software and of all the parents with internet access at home**,** just over half (54%) said that they had a filter installed.

While most said that they, or another adult, installed this software (78% of parents of 8-17 year olds), a minority (6%) said that their child did this. Responses from the children are quite different: 51% of children said that their parents or another adult installed the software, while 23% said that they or a sibling did this.

Figure 12 Who installed internet filtering software



Q: Who installed this software on your computer?
Base: All who currently have software installed on their home computer and use it: Parents of children aged 5-17 (282), parents of children aged 8-17 (237), children aged 8-17 (196)
Source: Ofcom – Children, Young People & Online Content, October 2007

Most parents do not think that their child knows how to override the filter (80% of parents of 8-17 year olds) – in contrast 67% of children said that this was the case.

The majority of parents are satisfied with their filtering software (88%).

The roughly one in five parents who have never used filtering software but are aware that it exists were asked why they don't use it. The reason most frequently given was that they trusted their child. This suggests that these parents think this type of software is used to *prevent* children from accessing certain sites/content rather then as a tool which could provide *protection* for the child. Other reasons mentioned were that their child was too young to surf/use the internet or that they did not think that they needed it.

Nine per cent of parents who had not previously been aware of these filters said that they would be interested in using them in the future, while the remaining 8% of all parents interviewed who had not been aware were not interested in using them in the future.

Forty-five per cent of all parents who use/whose child uses the internet are aware of other filtering systems, and of these just under half were aware (spontaneous) of the filters offered by their ISPs and just under one third of filters available on search engines .

4.8 Concerns about children going online and awareness of where to go to get help in protecting their child online

Attitudes to the internet [22]

The majority of parents agreed that they trusted their child to use the internet safely and that it was safe for them to go online ….

- 90% of parents agreed that they trusted their child to use the internet safely – 93% of children agreed that their parents trusted them to use the internet safely.

- 66% agreed that it was safe for children to spend time on the internet (15% disagreed) – 68% of children agreed and 12% disagreed.

…. and in general the children interviewed are more confident in their ability to manage their online risk than their parents are:

- 70% of parents agreed they know how to avoid online content that is inappropriate or harmful (18% disagree) – 82% of children agreed with this and 9% disagreed.

- 66% agreed that they know what to do if they come across harmful material online (19% disagreed) – 81% of children agreed with this and 10% disagreed.

However, the majority of parents have concerns about risks on the internet (especially regarding sexual content, paedophiles masquerading as children, child abuse imagery, and bad language). Children are, on the whole, less concerned about risky internet content than their parents:

- 89% of parents agreed that it is a risk that children may give out personal or private information online (however, as we saw above, just 14% of parents of 8-17 year olds spontaneously mention having rules around giving out personal information, indicating that this is not necessarily a top of mind concern).

- 81% of parents agreed that they are concerned that children might see sexually explicit images online (15% disagreed).

- 76% agreed that they are concerned that children might see violent images on the internet (15% disagreed).

- 53% of children agreed that they are worried about seeing inappropriate things on the internet (32% disagreed); 74% of parents agreed with this.

While parents overwhelmingly believe that internet users must be protected from seeing inappropriate or offensive content, slightly over half agreed that internet sites must be free to be expressive and creative:

- 91% believe that internet users must be protected from seeing inappropriate or offensive content

[22] All data in this section refer to parents of 8-17 year olds and children aged 8-17.

- 57% agreed that internet sites must be free to be expressive and creative, 20% neither agreed nor disagreed, and 18% disagreed.

Levels of concern

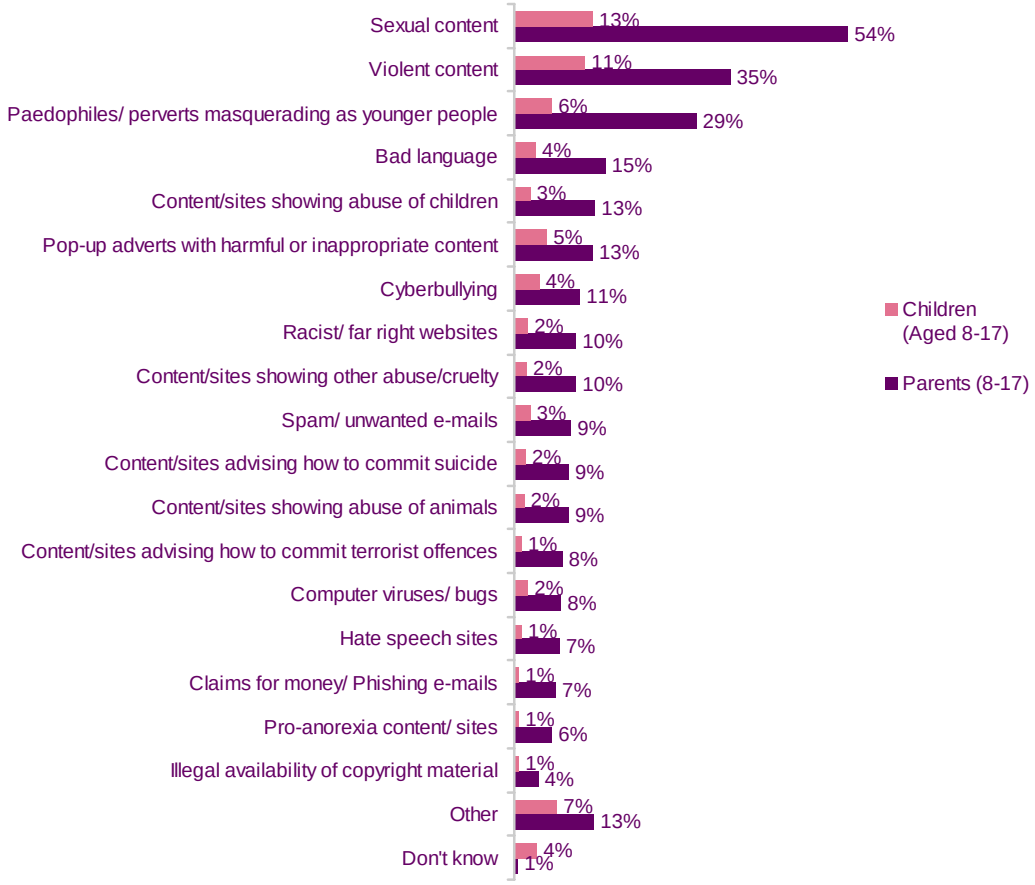
While the majority of parents clearly have concerns about the type of content/material on the internet, the reverse is true of children:

- 30% of children aged 8-17 said they had concerns overall, and 40% were very, or fairly, concerned.

- 66% of all parents said they had concerns overall, and 72% were very, or fairly, concerned.

Parental levels of concern about specific issues are higher than those of their children on all fronts, particularly regarding sexual content and paedophiles/perverts masquerading as younger people. Although parents are more concerned about it than their children, the gap between the responses of the two groups with regard to violent content is closer than for sexual content, and children are almost as likely as their parents to mention cyberbullying and pop-up adverts with harmful or inappropriate content:

Figure 13 Concerns about content on the internet – type of material: Parents vs. children



Q: What sort of things are you worried about?
Base: Asked of all who expressed concerns about content on the Internet and rebased on all parents/children
Source: Ofcom – Children, Young People & Online Content

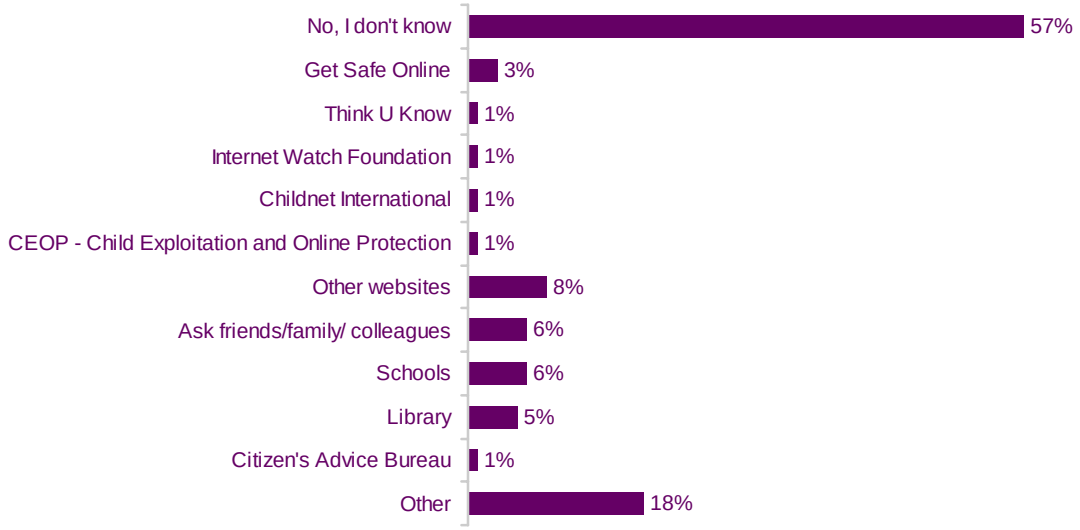
Although they have concerns about the types of content and material available on the internet, the majority of parents think the benefits of the internet outweigh the risks, and that real-life concerns like bullying and violence are more worrying. Children in particular agree with the latter statement:

- 60% of parents agreed that the benefits of the internet for their child outweigh the risks (18% disagreed).
- 56% of parents agreed that problems like bullying and violence in real life are more of a concern than inappropriate content on the internet (16% disagreed); 68% of children agreed and 11% disagreed.
- Parents are almost evenly split on being more concerned about harmful content on TV than online (34% agreed, 27% neither agreed nor disagreed and 37% disagreed).

Awareness of where to go to get help in protecting children online

Despite these high levels of concern, the majority of parents (57%) don't know where to go to get information to help them protect their child online:

Figure 14 Where parents get information to help them protect their children online



Q: Do you know where to go in order to get information to help you protect your child when online?
Base: All whose child uses the internet: Parents (621)
Source: Ofcom – Children, Young People & Online Content, October 2007

4.9 Children's exposure to potentially harmful or inappropriate content in the past six months

Level of exposure[23]

Despite the fact that the majority of children and parents agree that the child would tell a parent if they came across something that made them uncomfortable (85% of parents of 8-17 year olds agree with this and 87% of 8-17 year old children agreed), this does not always seem to be the case:

- Overall, 16% of 8-17 year olds said they had come across harmful or inappropriate material in the past six months, while 12% of parents of 8-17 year olds said that their child had had such exposure; a further 8% of parents did not know if their child had come across harmful or inappropriate content in the past six months. The likelihood of coming across such material increases with the age of the child, and the likelihood of the parent not knowing if the child has come across such material also increases with the age of the child.

- When questioned about 'nasty, worrying or frightening' material on the internet, 16% of children aged 8-15 questioned as part of Ofcom's 2005 media literacy research said they had come across such material, similar to the findings reported here.

Sexual content is by far the most frequently mentioned type of harmful or inappropriate content that is come across:

- Sexual content (mentioned by 67% of parents of 8-17 year olds versus 46% of 8-17 year olds)

- Bad language (8% each of parents and children aged 8-17)

- Paedophiles (7% of parents of 8-17 year olds, not mentioned by the children)

- Pop-ups (8% versus 12%)

- Violent content (7% versus16%)

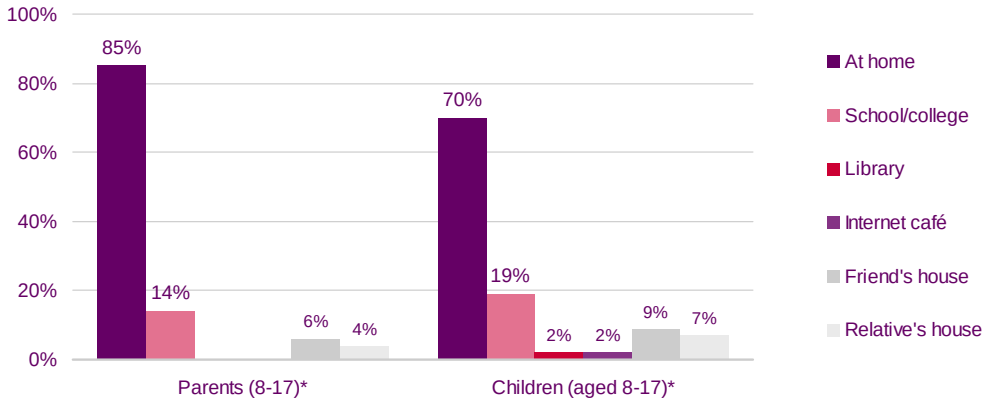
> The *UK Children Go Online* survey in 2004 found that 57% of 9-19 year olds who use the internet had come across pornography on the internet – ranging from 21% of 9-11 year olds to 80% of 18-19 year olds. This contact was most likely to come in the form of a pop-up advert (38% of all 9-19 year olds) or from accidentally going to a site showing pornographic material (36% of 9-19 year olds). The differences in the reported level of exposure between this research and the Children, Young People and Online Content Research probably stems from both a difference in how the questions were asked as well as the base of children from which responses were drawn.

Responses from parents and children indicate that most of this material was viewed at home, but children also say that this happens at school or at a friend's/relative's house.

[23] We asked first of all if they had come across harmful or inappropriate material in the past 6 months and if they had, we asked the open-ended question 'What type of content was it?'. Thus these findings relate to self-reported harmful or inappropriate material.

Parents seem to be less aware of out-of-home exposure to inappropriate content. This clearly has implications for the impact of rules on levels of exposure and risk.

Figure 15 Where children came across inappropriate content: Parents vs. children



Q: Where did they / you (children) come across this content / material on the Internet?
*Base: All who/whose child have/has come across harmful/inappropriate content on the internet: Parents of children aged 8-17 (62), children aged 8-17 (80), * caution – low sample size*
Source: Ofcom – Children, Young People & Online Content, October 2007

What children do when they come across harmful or inappropriate material

The majority of 8-17 year olds (87%) agree with the statement 'I would tell my parents if I came across something online that made me uncomfortable' and 85% of parents of 8-17 year olds agreeing that their child would tell them/their spouse if he/she came across something online which made him/her uncomfortable.

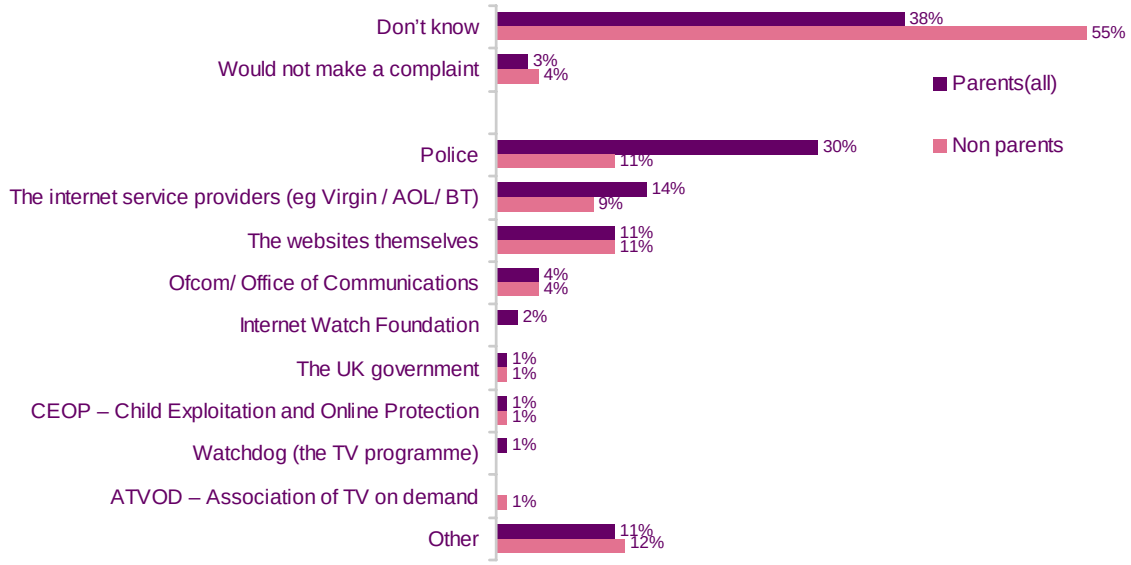
However, when children were asked what they did on each occasion that they came across harmful or inappropriate content, the net results[24] show that only 19% say they told a parent. Of course a reason for this could be that the material that the child came across, while considered harmful or inappropriate, either did not make them feel uncomfortable or they were not comfortable enough to share this with a parent. More children (40%) say they left the site immediately, or did nothing (21%). Compare this to parents responses where under half (44%) said they talked to their child about the material, 33% told their child to leave the site immediately and 24% say they made a complaint.

Those parents who did not make a complaint where asked why they did not.[25] The most common response was that they didn't know who to complain to, followed by the fact that they thought it wouldn't make any difference if they did.

A substantial minority of parents – almost four in ten – did not know who to complain to. Around a third would complain to the police, 14% to their ISP and 11% to the websites themselves. Most children say they would complain to their parents.

[24] Caution – small sample sizes as 16% of all children say they came across such material and 12% of parents say their child did.
[25] Caution – small sample sizes

Figure 16 Awareness of who to complain to about inappropriate content on the internet: Parents vs. non-parents



Q: As a general rule, who would you contact if you had a complaint about content / material you saw online that you considered harmful / inappropriate?
Base: Parents (653), non-parents (279)
Source: Ofcom – Children, Young People & Online Content, October 2007

Children were less likely to say they didn't know who to complain to, as the majority would turn to a parent – although this course of action tends to be lower for 16-17 year olds as they are more likely to mention the websites, ISPs and the police.

Mobile concerns felt by a minority of parents and even fewer children

All groups are much less concerned about harmful or inappropriate content on mobile phones. Those who said they had concerns mentioned similar issues to those on the fixed internet. 60% of all parents mention sexual content and 39% violent content. 29% of parents said they were concerned about bullying, 22% mentioned 'happy slapping' and a further 8% mentioned the misuse of mobile phones.

Section 5

A review of the literature on the risk of harm and offence on the internet

Ofcom commissioned Sonia Livingstone and Andrea Millwood Hargrave to update the literature review 'Harm and Offence in the Media', first published in 2006. The updated literature review focuses on TV, games, the internet and mobile phones. Annex 6 contains their full report ('Harm and Offence in Media Content: Updating the 2005 Review'). This chapter contains their summary and conclusions for the internet (which incorporates and updates the previous review) and their overall argument for a risk based approach to the issue of media harm.

Internet summary and conclusions

The evidence from this review on the potential harm from content provided through television and video games is clearly linked with the type of material contained in that content – for example, violent content or material that depicts sexist stereotypes and the potential effect that this may have on aggressive behaviour or on attitudes. Many researchers assume that similar effects will occur if the same material (from television, games or film) is encountered online, but this has not represented a distinct line of empirical inquiry.

Research conducted on the potential harm from online content includes some studies on the effects of viewing pornography or violent content, although, since the research is rarely experimental (i.e. controlling the content viewed), it is less clear exactly what content is at issue. Some researchers, however, are concerned that such online content is more extreme than that generally available on other media. Furthermore, the lack of clear definitions of levels or types of pornography, violence, etc on the internet, where the range is considerable, impedes research, as do (necessarily) the ethical restrictions on researching the potentially harmful effects of online content, especially but not only on children. Given these ethical issues, particularly when researching the risk of harm for children, there are difficulties in calling for more research here.

Despite the paucity of direct research on online harm to children (given practical and ethical considerations), there is a growing body of national and international research on children's distress when they accidentally encounter online pornography or other unwelcome content.

Most research regarding potential internet-related harm relates to risky contact rather than content, primarily that involving interaction with other internet users. Indeed, this update found a number of studies that addressed the risk of inappropriate contact (e.g. bullying - for which more research exists than for the first review, and also online contact with strangers). The research suggests that such contact may put users at risk of harm, either directly (as in meeting strangers in dangerous situations) or indirectly, from the consequences of their online behaviour.

It also appears likely that when children receive hostile, bullying or hateful messages, they are generally ill-equipped to respond appropriately or to cope with the emotional upset this causes; similarly, parents are unclear how they can know about, or intervene in, risky behaviours undertaken – deliberately or inadvertently – by their children.

Little or nothing is known about how young people respond to hateful content, especially in term of how the targeted groups (mainly, ethnic minorities) respond. Nor is much known regarding the use of niche sites – such as those that promote suicide or anorexia, though research is beginning to accumulate here.

Some phenomena are new since the previous Harm and Offence review, especially regarding the uses of social networking sites. Research on social networking sites has concentrated on the internet, although these are also available on mobile telephony as a delivery platform. For user-generated content, there is still little or no research. We have also considered excessive internet use ('addiction').

There are differences between the principal sites used – in the UK, Bebo (and then MySpace[i]) is currently more popular, while in the US much of the research has looked at Facebook, among others, partly because of its relative popularity, partly because US research tends to concentrate on university students (who use Facebook).

Research on the risk of harm has concentrated on social networking sites (raising issues of privacy) rather than on information uploaded onto user-generated content sites such as YouTube (n.b. these are increasingly populated by 'professionally' produced material).

For social networking especially, the issue of verifiability and anonymity is a problem. A significant proportion of young people communicates with strangers online and post material about themselves which would be considered 'private' in most circumstances. The ability to restrict access to sites is known about but not always used. Therefore, some young people knowingly give away inappropriate (private) information publicly (allowing access to 'anyone'). However, it seems likely that many more do so inadvertently, as a result of limitations both in internet literacy and in interface design.

This leads to concerns about the possibility of underestimating the unanticipated or future consequences of making private information public, especially since it appears that many young people have an inadequate understanding of the long-term consequences of publishing such information (e.g. employers are reported to look at social networking sites when considering employees).

The risk of inappropriate contact (especially in relation to sexual predation), harassment and bullying (including the easy dissemination of harassment or bullying content to others in the network) represent significant and growing policy concerns when considering the regulation of the internet.

Research suggests that young people may be aware of the risks, especially regarding social networking sites, but this awareness of the issues and problems is not always translated into action.

There is therefore growing evidence that, notwithstanding their many advantages and pleasures, social networking sites permit young people to create profiles that expose the individual or that ridicule or harass others, that using such sites for extensive periods of time (as is common) may isolate users of these sites from contact with 'real' people, albeit only for a few, addicted users.

In short, the widespread accessibility of the internet, along with its affordability, anonymity and convenience, appears to increase the likelihood of risk of media harm; although some argue that there is little new about online content, familiar content merely having moved online, most disagree, expressing concern about the accessibility of more extreme forms of content that are, potentially, harmful and offensive.

Does exposure to potentially harmful or inappropriate material lead to harm? The literature review identifies evidence suggesting some risk of harm. However**,** the evidence base is patchy and undeveloped and, for both practical and ethical reasons, some key questions remain difficult to research. The evidence that does exist points to the increased potential for harm online. Therefore research can only guide policy by supporting a judgement based on the balance of probabilities rather than on irrefutable proof.

A risk-based approach

While the concern of regulators is with harm, much of the research reviewed here deals with the risk of harm (by measuring incidence of exposure to risk, risky behaviour, or the use of certain media contents which may be harmful to some, etc.). Some of the evidence does demonstrate a link from exposure to 'actual' ill effect, although this is generally measured either experimentally in the short-term or by using correlational methods which cannot rule out all confounding factors. However, we note that the above definition of harm includes both potential and actual ill effects, and thus we discuss harm largely in terms of possible influences on behaviour and attitudes.

However, we argue also that the search for simple and direct causal effects of the media is, for the most part, inappropriate. Instead, we need an approach that seeks to identify the range of factors that directly, and indirectly through interactions with each other, combine to explain particular social phenomena. As research shows, each social problem of concern (e.g. aggression, prejudice, obesity, bullying, etc) is associated with a distinct and complex array of putative causes.

The research reviewed here and in the earlier review suggests that the media may contribute – more or less, under different conditions – to these complex social problems. A risk-based approach would take into account the range of relevant factors at work and allow for the possibility of their interaction. It should also weigh the relative contributions of different factors in explaining the outcome at issue, thus permitting a balanced judgement of the role played by the media on a case by case basis.

We therefore call for more research that will put possible media effects in context, seeking to understand how the media play a role in a multi-factor explanation for particular social phenomena (e.g. violence, gender stereotyping, etc), including an account of the relative size of effect for each factor so as to guide regulatory decisions based on proportionality.

Section 6

What can be done to help children, young people and parents manage the potential or actual risks of going online

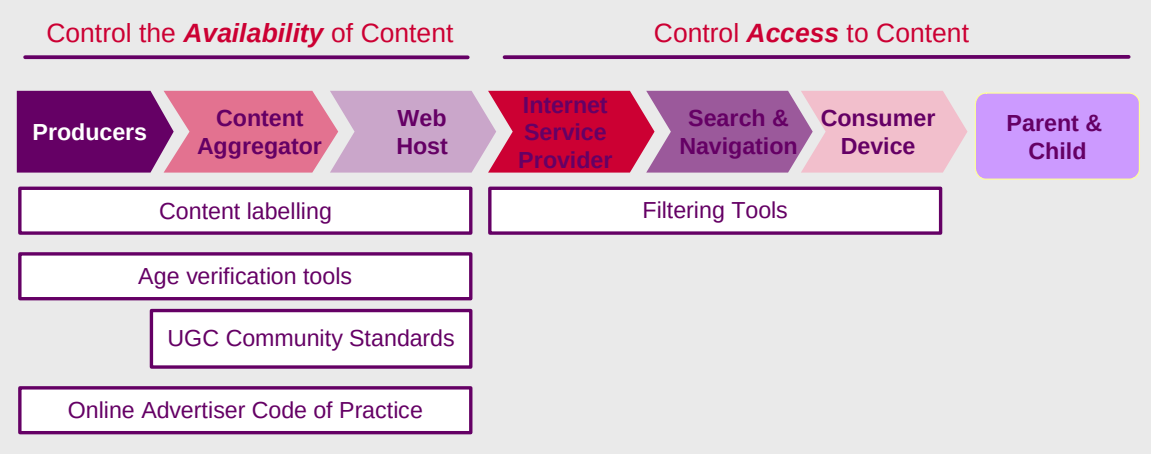
In this chapter we identify the areas where specific actions might be considered, building on a map of existing UK activity and on lessons from other regions. Ofcom does not comment on the issues relating to the sale of games for PC and games consoles, though the measures we discuss below will contribute to the management of harmful content in games played online.

The key findings from this chapter are as follows:

The research findings reported above, and the overall conclusions from the literature review, suggest a lack of evidence for actual harm, but evidence for the risk of harm, We can conclude from this that there is a case for considering what could be done to help children and parents manage the potential or actual online risks.

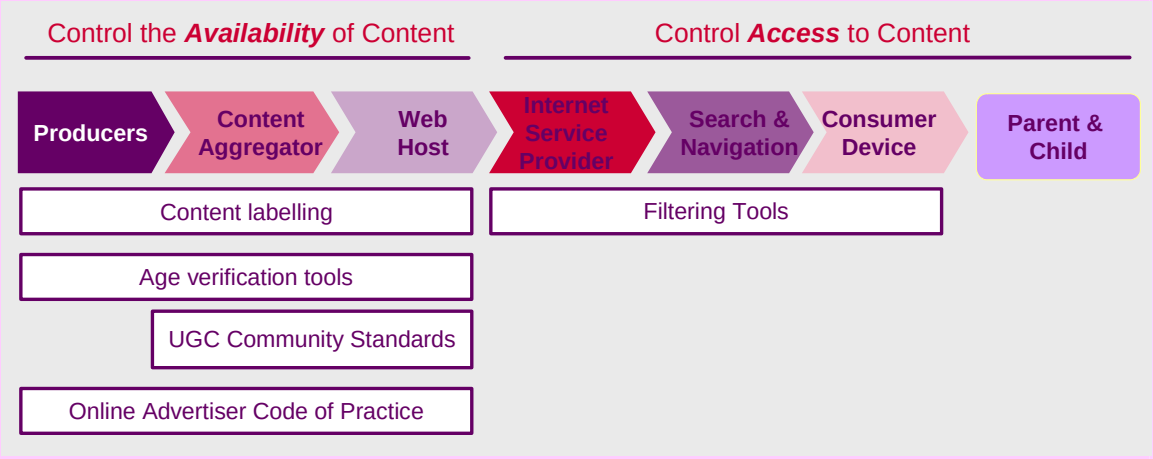
The current legal constraints and problems of jurisdictional reach mean that statutory regulation is not possible for key parts of the value chain and, even if adopted as an approach for the parts where it is feasible, would be of limited effectiveness. This is, in large part, because the internet is an open global platform, and statutory regulation can only have national reach – unless the regulation also involves curtailing the openness and global reach which distinguish the internet from traditional platforms and are the basis of its impact and value.

Therefore a new approach to content regulation is needed, one which is built on a model of distributed across the value chain, relying much more on personal responsibility and on industry self-regulation than on traditional, formal intervention.



Our suggestions involve, for the most part, a refocusing or widening of activity that is already under way in the marketplace: we are not proposing new regulatory interventions; rather, we are taking those that the market and/or Ofcom has already recognised and promoting the best of them.

Our analysis employs a value-chain model of the internet content market: we consider what different contributions industry players at each stage of the value chain can make. In the self-regulatory context we have described, these industry contributions are typically aimed at empowering or enabling parents and children to manage their content experience, and in particular to avoid potentially harmful content.



It is our view that, taken together, the combination of enhanced media literacy skills on the part of parents, children and young people, and targeted industry, NGO, regulatory and government initiatives, will help deliver an environment in which:

- parents are more confident of their ability to support their children online; and
- children themselves are confident in their online e-safety and also know what to do when they come across material that is potentially harmful or offensive.

We would encourage the Byron Review team to consider what success would look like. This could frame a further review within two years of implementation of the recommendations, asking:

- Whether there are any further learnings regarding the evidence of harm and the level of risk which should be taken into consideration;
- Whether satisfactory progress has been made in relation to the concerns raised and if not, whether alternative measures need to be pursued.

6.2 Does more need to be to done to help children, young people and parents manage the potential or actual risks of going online?

The internet raises some new challenges for societies which have previously been able to regulate, to a significant extent, the media to which their citizens are potentially exposed. The internet is a global medium, through which it is easy for individuals as well as businesses to offer content and services to a global audience. In relation to a specific concern – over the types of content to which children in the UK might have access - we face a potentially unlimited number of originators of content, operating from territories often outside our jurisdictional reach, and where standards of legality or acceptability may be different to those in the UK.

As seen in chapter 4, our research with parents, young people and children[26] shows that while they have concerns about the internet, for most, the benefits outweigh the risks. That said, a mixed picture emerges regarding the degree and effectiveness of parental oversight of internet use at home, almost one in seven children aged 8-17 say that they have come across potentially harmful material in the past 6 months, and the majority of parents do not know where to go to get information about how to help protect their children when online.

A review of the literature[27] - summarised in chapter 5 - identifies evidence suggesting some risk of harm. However, the evidence base is patchy and undeveloped and, for both practical and ethical reasons, some key questions remain difficult to research; the evidence that does exist points to the increased potential for harm online. Therefore, research can only guide policy by supporting a judgement based on the balance of probabilities rather than on irrefutable proof.

The research findings reported above, and the overall conclusions from the literature review, suggest a lack of evidence for actual harm, but evidence for the risk of harm, We can conclude from this that there is a case for considering what could be done to help children and parents manage the potential or actual online risks.

In developing our suggestions for the Byron Review team to consider as it develops its own recommendations, alongside the research and literature review discussed above, we have also undertaken a review of the operation of the internet content market[28], the legal and regulatory frameworks affecting internet content in the UK[29] and in a range of other regions of the world[30], as well the range of existing means through which children are protected[31] (there is already a great deal of activity, by service providers, government agencies, charities, and parents, seeking to address this goal).

In considering what more can be done, we also note the limitations on the extent to which internet risks can or should be addressed through traditional regulatory interventions.

Before considering the alternative ways in which the risks to children can be addressed, it is necessary to clarify the different forms of potentially harmful content which create such risks, and the circumstances through which such content becomes available to children. There are two distinct areas of harmful content which have led to concerns in the UK, which may require distinct solutions, and which have been tackled in different ways in international markets. These are:

[26] See Annex 5
[27] See Annex 6
[28] See Annex 1
[29] See Annex 2
[30] See Annex 4
[31] See Annex 2

- illegal content, which is unacceptable for all, and may present risks of harm to adults as well as to children – such as abusive images of children, sexual violence, or material encouraging race hate; and

- content, the publication of which is not illegal in itself – i.e. that is appropriate for adults but not for children, such as non-illegal sexually explicit or violent content; or that which depicts dangerous or illegal activity, such as fighting among children (and happy slapping), gang membership, etc.

The Byron Review's remit, and the focus of this report, is on the risks associated with legal but harmful content; we also provide an account of the ways in which illegal content is tackled in Annex 2.

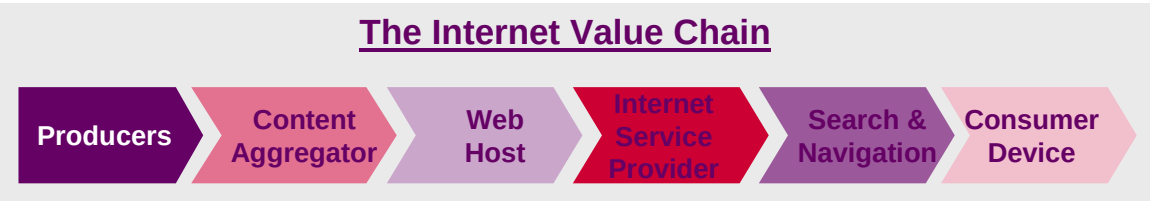
6.3 Traditional content regulation and regulation of the internet – why a new approach is needed

This section proposes that harmful content on the internet must be addressed in a different way to the historic models of content regulation, exemplified by the broadcasting market. The analysis below suggests that, in contrast to the broadcasting market, the responsibility will be shared, and that the part played by statutory regulation will be negligible. Many discrete activities will contribute to the increased safety of children online, but there is no one institution which can act as the channel does for broadcasting: as the locus of responsibility for content standards.

While there is a wide range of activities in the broadcast market (e.g. producing programmes, operating channels, running platforms like Sky or Virgin Media, producing and distributing consumer equipment like television sets and set-top boxes) for the purposes of controlling harmful content, regulation focuses exclusively on channel operators, who are bound to conform to national standards in relation to the content which they offer. The content available to UK audiences is managed through a bilateral relationship between regulator and channel operators. The position is very different in relation to the internet.

We use a model of the internet value chain to illustrate the key distinctions (further detail is available in Annex 1):

Figure 17 The internet value chain



The critical feature of the internet value chain is the fact that all but one of the activities are outside individual nations' jurisdictional reach: content creation, content aggregation, hosting, search and the consumer device (software and hardware) are all global markets. These products and services are outside the specific control of individual nations or even trading blocks. As a consequence, national (UK) legislation or regulatory initiatives cannot be expected to be an effective means of managing UK audiences' access to media online – content providers who don't want to comply with UK rules can easily operate outside the UK.

Uniquely, providers of internet access (ISPs[32]) are entirely within national jurisdiction: UK internet access providers are physically located in the UK, and therefore represent the sole means through which it might be possible to control the distribution of potentially harmful content in the UK; in other words, to play the role which channels play in broadcasting.

However, regulation of internet content via ISPs, for the purposes of controlling national internet content markets, is an undesirable and inappropriate response to the risks of harmful content. (As discussed in Annex 4, in a small number of nations, including China, and Saudi Arabia, the internet content market is controlled through ISPs regulation).

The legal context: ISPs

The debate over the role of the ISP has already been had at the EU and UK level in the context of the Electronic Commerce Directive (the "Directive")[33] as implemented in the UK in the Electronic Commerce (EC Directive) Regulations 2002.[34] This framework limits the liability of service providers who unwittingly transmit or store unlawful content provided by others in certain circumstances.

For our purposes, there are two critical categories of service provider that are granted specific protections from liability in relation to illegal content: those who transmit information (i.e. 'mere conduits'), and those engaged in 'hosting' information.

ISPs will typically have protected status under the Directive because they are likely to be 'mere conduits'.[35] Where they do not initiate the transmission of content, select the receiver of the transmission, or select or modify the content transmitted, they will not have legal responsibility even where that content is unlawful. The Directive also prevents Member States, including the UK, from imposing general obligations on such service providers, to monitor the content they transmit or store.

The existence of a current legislative constraint is not a sufficient reason to reject consideration of ISP regulation in the future. However, Ofcom considers that ISP regulation is unlikely to be an appropriate mechanism to control internet content markets for the following reasons:

Firstly, the basic 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.

Finally, there is a practical consideration: what exactly it might be that the regulated ISP should do? In the context of the Byron review, our concern is with content which does not break the UK's existing content rules – and in the law, is acceptable for adults. In some countries which do control internet content through the regulation of ISPs, this distinction is

[32] Such as BT, Virgin Media, Tiscali

33 Directive 2000/31/EC

34 SI 2003, No 213.

35 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.

less important: ISPs are used to control the accessibility of a very broad range of content defined as illegal.

Requiring ISPs to take responsibility for controlling children's access to content acceptable for adults, but potentially harmful to children, would in effect transform an ISP into something much more like the operator of a broadcast platform; ISPs would be incentivised to carry content exclusively from recognised or approved providers. This regulated platform would not be the open and innovative internet available today: if ISPs blocked unknown content they could prevent the development of new products and services.

Finally, it is important to note that although no legal duty applies, ISPs in the UK and many other regions already make a significant contribution to the management both of illegal and harmful content. The role that ISPs play today, and the extent to which they might play a greater role, is discussed below.

The legal context: hosts

The UK and EU legal framework also protects those providing internet hosting services from liability for illegal content in certain circumstances. Internet hosts are defined as those who store third party information, and they have a partial protection from liability – they are not liable for hosting content which is illegal, until they have "actual knowledge" of illegal activity or information. This protection from liability ends when they do have actual knowledge, unless they act expeditiously to remove or disable access. As with conduits, member states are prohibited from imposing monitoring obligations on hosts.

These protections are important, because there is a broad range of providers of hosting services: in particular, user-generated content hosts like YouTube (and thousands of others) are typically classified as hosts under the legislation and are therefore protected in respect of illegal content liability, and protected from the imposition of monitoring duties. Since hosts are also part of the global market any national initiative focusing on the actions of hosting service providers would in any case have limited impact on the totality of inappropriate content available to children.

6.4 Self-regulation, self-organisation and consumer responsibility

If no individual institution or set of institutions can be charged with responsibility for managing the risks to children of exposure to harmful content, what can be done? The answer is that harmful content risks must be approached as a distributed responsibility. Under this model everyone has a role to play, but none is uniquely in a position to promise safety. Put another way, the familiar assertion "You can't regulate the internet" is both true and misleading: the internet can't be regulated like broadcast television – if it could it wouldn't be the internet as we know it; but a wide range of actions can help restrict the accessibility of potentially harmful content to children, even if there is no statutory regulation involved.

This important conclusion also raises some issues: where there is distributed responsibility, individual players in the content value chain may seek to evade individual duty, even though each has an important role to play. Furthermore, it is difficult to ensure that a system of distributed responsibility is effective, because statutory duties will play a minimal role. In other words, if the UK is necessarily limited in the extent to which it could regulate global content producers, search providers, internet hosts etc; and if the regulation of ISPs is not an appropriate solution either, the UK must inevitably rely to a greater extent on *self-regulation* or *self-organisation*[36] (respectively, through joint action by industry players or the individual

[36] Self-organisation refers to individual corporate initiatives which seek to address a public policy goal

efforts of single businesses) to help secure the protection of children. In fact this approach is recognised by the E-Commerce Directive; there is a specific obligation on Member States and the European Commission to encourage the drawing up of codes of conduct, including in respect of the protection of minors and human dignity.[37].

This has two important consequences: firstly, as is typically the case when a self-regulatory model is adopted to address a policy objective, a greater degree of responsibility will rest with consumers; and secondly, that in considering actions through which children's safety may be enhanced, it is necessary to pay careful attention to the extent to which industry commercial incentives are aligned with the interests of citizens and consumers. Where incentives are not effectively aligned, either in terms of individual incentives of a company or the collective incentive of industry to support public commitments, then a self-regulatory model is less likely to be effective. In examining the current and future roles we can expect of industry, we therefore give careful consideration to the extent to which corporate incentives would be likely to support industry action, either by the most significant individual players or by the majority.

Furthermore, it is important to recognise the extent to which the regulated broadcast market also relies upon parents' actions. Broadcast TV includes a great deal of potentially harmful content; the system relies upon parents' awareness of the watershed, and their ability to respond to on-air warnings, programme titles, and to the context provided by channel brands to manage their children's media experience. Harmful content on the internet creates new duties for parents, but their central role in protection is characteristic of the more highly regulated TV environment.

As discussed in Annex 2, industry players across the value chain already make important efforts to support people in managing online risks effectively. There are some opportunities where industry might contribute more to supporting children in the online environment, which we describe below. However, some of the most significant opportunities to improve children's safety in relation to inappropriate content are through the development of children's and parents' awareness of the risks, and their ability to manage them – not though traditional regulatory interventions, which focus on changing the behaviour of industry players through statutory direction.

The significant role which consumers play in managing harmful content risks is the subject of subsection 6.3; subsection 6.4 examines the current contributions to protection, the further roles which industry might play, and the mechanisms through which they might be incentivised to do so.

37 Article 16(1)(e).

6.5 Individual responsibility – the role of parents, children and young people

In order to help people take more personal responsibility when they go online, we need to help them become more media literate. Media literacy is the ability to access, understand and create communications in a variety of contexts. Some call this 'literacy for the twenty-first century'. Put another way, if literacy is not only about reading and writing, but also about comprehension and critical thinking, then media literacy is about engaging these capabilities when using and consuming media. Without media literacy, people's ability to participate effectively in society, the marketplace and in the workforce may be greatly diminished. The remit of the Byron Review directs our attention principally to issues related to access – how to find the content and services wanted and how to avoid the content which may be potentially harmful or offensive – and indeed this is the focus of our response. However, Ofcom also recognises the importance of 'understanding' and 'creating' in the broader media literacy landscape, and these latter aspects are a part of our overall media literacy work programme.

The evidence clearly points to a need to help parents, children and young people manage the potential or actual risks of going online, by improving their media literacy skills. We suggest a focus on the following media literacy outcomes to help parents, children and young people manage the potential or actual risks of going online:

Outcomes:

- Increased awareness and understanding among parents of their critical role in ensuring the safety of their children when they are online, through the effective application of carefully targeted and age-appropriate rules.
  For example:
  - Increased parental awareness of where to go to get information on protecting their child online as well as tips to ensure that the child has understood and accepted the importance of any rules that the parent puts in place (e.g. an internet green cross code).
  - Increased parental understanding of how they can apply their real-world parenting skills to the online world (i.e. it's not necessarily just about technical literacy).
  - Increased parental awareness of what children are doing online more generally and the key areas/things that they need to look out for.
  - Increased awareness of the age-appropriateness of certain activities online, e.g. using a social networking site (SNS).
  - Increased parental and children's awareness of the risks of children's content access and other online activity (e.g. privacy in relation to the personal information that children share about themselves online) as well as child contact.
  - Increased awareness of where to find high-quality content online, for younger children in particular.

- Increased take-up of content management tools such as filtering software, by making parents aware of its existence, its benefits and its limitations.

    - Increased use of other forms of filtering, such as those provided by search engines.

    - Increased awareness and understanding of the tools provided by parents' ISPs and awareness of those ISPs which are more 'family-friendly'; for example, as demonstrated by the presence of a family-friendly 'trustmark'.[38]

- Increased awareness and understanding of the meanings of the content labels used by industry as well as the implications of these in relation to children's use of content.

- Increased awareness of where to complain about potentially harmful or inappropriate content online – e.g. IWF for illegal material, the site host for inappropriate material, their filtering product provider where they identify over- or under-blocking.

- Increased awareness among parents and children of the role that they can play, both in labelling the content they put online and in 'community policing'.

- Alignment of the advice and information that is being given to parents, teachers and children.

    - Integrated awareness-raising and educational initiatives, targeted at parents, teachers and children, at a local and national level, for maximum effect.

    - Linked to this, the inclusion of e-safety across the national curriculum from a younger age

Delivering these outcomes

A very broad range of good initiatives are currently under way in this area – from those associated with formal government agencies such as Becta and CEOP, to those offered by charitable organisations, industry bodies and individual industry players including organisations such as Childnet International, Media Smart, the BFI, the Media Literacy Task Force , the BBC and Channel 4[39]. However, to deliver the outcomes offered for consideration above, we propose that thought is also given to the following:

- The development of a framing strategy for the delivery of the above outcomes – across the various government departments, industry bodies and individual industry players, charitable organisations and regulators - with a single point of oversight and coordination

    - Development of short-, medium- and long term targets and the identification of the communications plan, educational initiatives and funding necessary to deliver these on a sustainable basis.

        - Consider the appropriate balance between a high level public information/awareness campaign and on-the-ground activities
        - Prioritise the more vulnerable children.

38 See below, 'The promotion of industry self-regulation' for more on this.
39 See Annex 2, for more details

- Creation of communications and materials that are target-group specific, i.e. tailored to the different types of parents, children and teachers so that they are appropriate to the level of the recipients' skills and understanding.

- Explore potential for cross-government and industry funding.

The development of such a strategy could consider the lessons learned from similar initiatives in other countries. For example, in France, the national CONFIANCE project is based on co-operation between the government ministries, educators, technology providers, and a wide range of other players, including public institutions, NGOs and private companies. A key aspect of the project is a national awareness campaign 'Internet sans Crainte' – 'Internet without Fear' which aims to reach a broad variety of target audiences and makes use of existing initiatives and materials. Other nation-wide initiatives in France include a media campaign orchestrated by the Interdepartmental Delegation on Family Matters, across all public media, and a national educational plan to raise awareness of internet safety issues among students and educators. In Sweden the Swedish Media Council has developed a standard tool-kit of materials which is being implemented though regional training workshops with educational professionals, social workers and welfare officers across the country.

- The development and promotion of an easy-to-use and interactive online 'one-stop-shop' for information on how to protect children online to help parents, children and teachers. For example:

  - FAQs

  - Help

  - What's new

  - Safety forum

  - Advice on the tools available – e.g. filters, labelling, how to complain, family-friendly ISPs etc.

  - Age-appropriate internet 'green cross code'

  - Where to complain

  - Links to other relevant websites

  In this area too, international examples may be useful. One example is the Australian Government's *NetAlert* programme, which, as part of broader range of activities, provides a central website[40] containing information on internet safety issues, free software tools, and links to interactive educational environments. These include the *Cybersmart Detectives* game that teaches children key internet safety messages - the activity is based in the school environment, and brings together a number of agencies with an interest in promoting online safety for young people. *Netty's World* is another example of an interactive learning environment, and is designed for young children (aged 2-7) to learn about

40 http://www.netalert.gov.au/

internet safety issues. *NetAlert* encourages parents to take their children through an online storybook where safety messages are revealed through five adventures. Children can also join *Netty's Club* in which offline internet safety activities (such as bookmarks, stickers and pencil holders) are sent free by post.

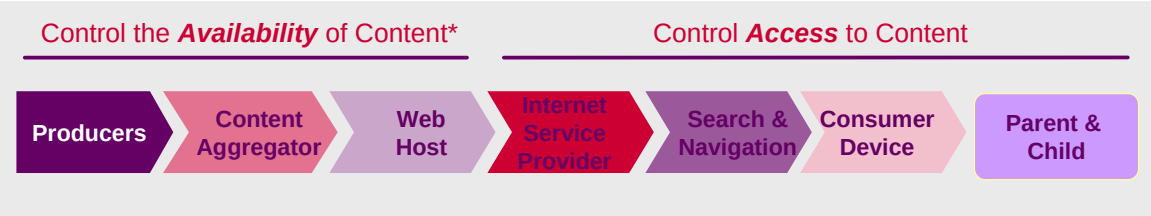
We have outlined our thoughts on the desired ends and described some of the possible means, but there is still a substantive question outstanding: what should be the institutional mix to make this happen (i.e. what is the role for Government, Ofcom, the BBC, schools, CEOP, industry etc.), as well as the appropriate funding model.

6.6 Industry and the management of harmful internet content

For the purposes of this analysis, it is most useful to think of two broad groups of activity in the value chain:

- content creation, aggregation and hosting are the activities through which content is made *available* to the global audience, and to UK children in particular;
- internet access, search, and the consumer device (software and hardware) are the means through which the content is *accessed* by those audiences.

Figure 18 The internet value chain: controlling availability and access to content



In considering industry actions through which greater protection from harmful content can be secured for children, there are two broad types of intervention: those intended to affect the extent to which content is made *available* on the internet; and those intended to affect the extent to which the content is *accessible* to (vulnerable) audiences.

UK initiatives intended to control the availability of potentially harmful content will tend to be limited in their impact to businesses which are within the UK's jurisdictional reach. However, actions developed in collaboration with industry can have a broader impact: corporate 'good citizens' outside the direct jurisdictional reach of the UK may still be inclined to comply with UK standards, guidelines, codes of practice etc., where these are also consistent with their businesses' successful operation.

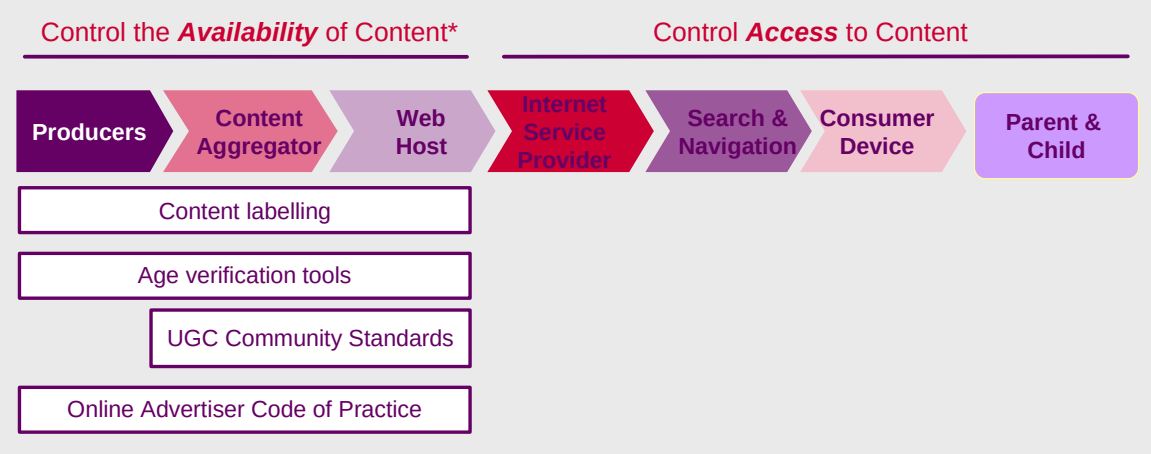
Activity intended to control access to content can potentially extend to services from anywhere. In considering how to manage content risks we will consider first the extent to which the *availability* of harmful content to children can be managed, and what opportunities exist to secure greater protection, and then examine opportunities in relation to controlling the *accessibility* of such content.

Controlling availability

As noted above, content producers, aggregators and hosts all operate in a global market, and the potential reach of UK initiatives to manage access will necessarily be limited. However, action at these points in the value chain can nevertheless make a significant contribution to the protection of children from harmful content.

There are four broad means through which the *availability* of harmful content can be managed:

Figure 19 The internet value chain: controlling availability to content



- Content classification and labelling: providers can offer information about the characteristics of their content to inform audiences about the nature of the content. Users can refer to this information directly – as is the case with labelling systems like the BBFC movie ratings, or the PEGI video games ratings systems – or indirectly via filtering and search and navigation tools which refer to labels to identify content unsuitable for children.

- Age verification: content providers can restrict access to content inappropriate for children through the use of tools to establish users' age. A credit card number is the most widely used age-verification tool.

- UGC Community Standards: The emergence of online communities is a central feature of the internet content environment; user-generated content hosting sites, such as YouTube or DailyMotion, social networking sites (SNS) and peer-to-peer (P2P) communities all allow individual audience members to upload and to share content with other members of the community (though in the case of P2P communities this is often copyright content). These sites cannot rely on the top-down forms of content management because their users determine what the site comprises: they are hosts, as defined above. However, communities typically have 'site standards' which define the types of content users are encouraged to share; and the categories of content that are forbidden. Many of these sites operate community-led review processes to ensure that content on the site fits the site standards: users can complain about individual content assets, and the site operator commits to reviewing the content and remove it in the event that it does breach standards. Annex 2 includes more details of such sites and review processes.

- Advertising content controls: These present an indirect means for addressing potentially harmful content. For the most part, content which is made freely available

online relies on advertising funding; through codes of conduct, and other means, advertising flows to the providers of harmful content can be restricted. In the UK, the Internet Advertising Sales House (IASH) code of practice defines types of websites prohibited for its members' adverts, as well as websites where IASH members need to seek permission from the client before placing an advert. Other controls include codes of conduct set by affiliate networks and restrictions placed by Google AdSense (described in Annex 1).

Content classification, labelling and tagging

In general, content providers are in a position to classify their content – to decide whether it is for children or adults; is funny or frightening; is a cartoon or reality footage etc. Content providers can attach information 'labels' to classify their content. In general, a content provider has strong incentives to provide accurate information about the characteristics of the content they are offering, whether it is a website or an individual piece of content. It is this information which enables interested audiences to find content: and unless a user knows something about what to expect, there is no reason to look at a given piece of content. In principle, we should expect all content to have some kind of label or content information. However, there is a significant gap in the application of standardised labels like the ICRA framework[41] or the RTA[42] label, which can be used to manage or control access to specific types of website.

Despite the easy availability of such frameworks, the application of standardised labelling remains negligible. Most importantly, this is because the incentives to adopt *standardised* labelling tools for content producers are generally low (unless producers are required to do this as part of commercial agreements). This is, in part, because standardised labelling tools are not widely used for content filtering – reinforcing the lack of incentive for providers.

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 use in blocking lists. The report concluded that "*voluntary self-labelling cannot provide a solution to tackle the problem of unlabelled web pages, except if labelling becomes compulsory*".

In practice, creating a statutory duty requiring content providers to label for the purposes of content filtering would be ineffective – it would be impossible to enforce for non-UK sites, and impractical in relation to the thousands of UK individuals who make their own internet content available. In particular, it would create a duty and potentially a liability for UK citizens and content businesses, while allowing providers of potentially harmful content, such as pornography, easily to evade the requirement, by operating outside the UK.

Although a general requirement for labelling for the purposes of content control may be impractical, there is a role for labelling frameworks in content sub-markets for commercially-produced video (such as TV programmes) and films, especially those which are potentially harmful.

41 This is a simple labelling framework supported by the Family Online Safety Institute
42 Restricted To Adults (RTA) is a label recognised by a broad range of filtering products; it is intended for all content inappropriate for minors, though mainly is use by pornography providers

Option for consideration:

There are two policy initiatives currently under way in the UK which could enhance the breadth and effectiveness of content labelling in relation to commercially produced audio-visual content. We recommend the Byron Review team considers promoting and supporting the efforts described below to improve the quality of content information in relation to audio-visual media.

- The Broadband Stakeholder Group, supported by Ofcom and key industry players, is developing a common framework for the ways in which viewers should be informed about commercially produced audiovisual content that is potentially harmful or offensive. These common principles, once agreed by industry, will form the basis of good practice in enabling viewers to protect themselves and their children from exposure to such content.
- Looking forward, the new Audiovisual Media Services Directive requires the UK create a new regulatory framework for on-demand television service providers, including those operating on the internet. The UK is in the early stages of developing this model; however, effective and consistently applied content information is likely to be a significant element of the framework, along with other measures to control children's access to harmful content familiar from broadcast markets – such as PIN controls.

Critically, these initiatives focus on behaviour which is aligned with the interests of industry players. Mainstream content providers will benefit from being able to provide their audiences with a predictable, managed content experience. Application of these frameworks can rely on a UK self-regulatory framework (or co-regulatory, where required under the AVMS Directive). Some operators may wish to avoid such a framework – however, adoption of a stricter statutory model would have limited impact, as non-compliant operators are free to base themselves outside the UK.

There is a further means through which content labelling and classification can contribute to the management of harmful content of all kinds: through the operation of audience participation in classification.

Content classification by members of online communities of interest is an important part of the process for managing potentially harmful content in community environments. In practice, a user posting material onto a user-generated content site can be presented with a range of means to label their content. The user will always be able to add "tags", to which other users can refer in order to inform their content choices; in some instances they can add standard labels – categorising content as entertainment or music; or indicating that content is inappropriate for children.

More broadly, members of the audience can themselves label content in certain environments. In relation to potentially harmful content, audiences can work with providers of filtering services, alerting them to instances of incorrectly classified content (over-blocked or under-blocked). This option is discussed below in the subsection on filtering.

In the longer term, members of the UK and global audience represent the most significant resource in developing effective, accurate and usable content information. Services like the photo-sharing site Flickr derive their value in substantial part from the actions of users in 'tagging' content with labels – ensuring that other users can find exactly what they are looking for. The more widely the internet audience takes responsibility for sharing information in this way about content which is good or harmful, or which is relevant to

specific audience groups, the easier it will become for individuals to find the content they want, and to protect themselves and others from the content they wish to avoid**.**

UGC community standards

There has been considerable media and political attention paid to the availability in online communities of potentially harmful content; particular attention is focused on the availability of content on YouTube which is:

- appropriate for adults but not for children; and
- undesirable but not illegal, for example material which depicts dangerous or illegal activity, such as fighting among children (and happy slapping), gang membership etc.

It is important to note that the specific attention paid to YouTube, and to other market-leading providers of UGC hosting like MySpace, is based not on the fact of their providing UGC hosting services, but on their market-leadership position and the fact that they offer a general use proposition: they are targeted at adults *and* (older) children. Public concern does not seem to be directed at the large numbers of UGC-hosting services whose stated objective is to enable communities to share pornography (YouPorn.com, PornoTube.com), violent content (Extremevideos.org; Almostkillled.com), whose content clearly creates a risk of harm for children, or illegal copyright content (thepiratebay.org; and the recently closed Demonoid.com).

YouTube, and the other major UGC hosts, typically operate two mechanisms through which children's access to potentially harmful content can be controlled: a form of age verification, discussed below; and community standards processes – under which:

- the site defines a standards framework – for example YouTube includes the guideline *"YouTube is not for pornography or sexually explicit content.*" In contrast, Pornotube requires only that content posted is legal;
- users of the services can flag videos – indicating that they believe a specific video does not comply with an aspect of the community standards framework; and
- the service operator will review the item against its community standards framework, and, if it agrees with the user's judgement, it will remove the video from the site. In some instances respected members of the community are also empowered to review and remove content which is of concern.

In principle, these systems should ensure that content is compliant with the site's terms of use - though for some services these will of course include or encourage the posting of potentially harmful content. There is nothing that can be done to address the *availability* of such adult-targeted (harmful but legal) services operating from outside the UK. The *accessibility* of such services to children can be addressed through the use of filtering solutions, discussed below.

However, there remains a real distinction between mainstream hosting providers and harmful content communities, which is that mainstream services are intended for the use of children as well as adults: and this is reflected in the top 10 ranking among children of these types of service[43].

[43] Neilsen Online, August 2007. See Annex 5

Many commentators believe that the review processes on mainstream sites are ineffective, and that they allow content which contravenes guidelines to remain available; and there is anecdotal evidence supporting this hypothesis. It is, unsurprisingly, possible to find content on mainstream sites like YouTube which might appear to be inconsistent with site standards. (Access to content which is assessed as consistent with site standards, but intended for adults only, is controlled through a limited form of age verification, discussed below).

Unfortunately, it is not possible to determine empirically how effective site review processes actually are. Major UGC sites often operate sophisticated review processes: YouTube offers multiple categories under which content can be flagged (including sexual or violent content; and subcategories, like "physical attack" or "minors fighting"); and allows an escalation process in the event that a complainant is unsatisfied, but there is no transparency over the operation of the process. Although YouTube, for example, commits to reviewing all flagged content within 48 hours, the process remains opaque to the public. Furthermore, because it is impossible to determine what proportion of content is potentially harmful, there is no means to assess the overall effectiveness of the system. In the absence of transparency, and given the evidence of individual instances of potentially harmful content, the continued expressions of concern among policymakers and others are understandable.

It is important to distinguish between the distinct types of content which might create such concerns: content which is illegal in the UK; content which is potentially inconsistent with site standards; and content which is legal but may only be appropriate for adults.

Although illegal content is not our specific concern in this report, it should be noted that YouTube, among others, already provides regionalised versions of its service in response to direction from individual nations about content which is illegal under national law. National law enforcement agencies are able to inform YouTube of locally illegal content. If it is inconsistent with site standards, it will be removed; if consistent with such standards it is retained for the rest of the world, and removed from the version of YouTube offered in the country where it is demonstrably illegal.

In relation to content which is legal in the UK, the UK does not possess any powers which would enable it to require YouTube to adopt different content standards or a different content review process to that which currently exists. The E-Commerce Directive imposes an obligation on Member States and the Commission to encourage voluntary codes of conduct regarding the protection of minors and human dignity. The self-organisation scheme which YouTube already operates is clearly intended to ensure that the site's content is consistent with the content standards it defines.

What remains unclear is what relationship exists between the self-organisation scheme principles and the specific timetable commitments YouTube makes to community members, and the actual operation of the scheme.

Option for consideration:

We recommend the Byron Review team considers working with industry to create a voluntary scheme or code under which UGC providers make transparent the operation of their content review processes – for example, reporting on the turnaround times for these processes, on the timetable (if any) for communicating with complainants, and ideally, with independent verification of performance

This type of scheme could mirror the commitment concerning complaints' handling process made by Facebook to the New York Attorney General to determine their response to any complaints about sexually explicit content within 72 hours of receiving the complaint.

It is not wholly clear what the architecture of incentives is, in relation to this idea. Facebook's commitments emerged from direct intervention by the attorney general, as opposed to pressure from audiences. Successful mainstream UGC hosts would argue that their sustained growth, and popularity across all population groups, is good evidence that their current approaches to content control are effective, and that audiences' interest in greater transparency is limited. However, to the extent that greater transparency about the sites' content review processes may reassure some users (parents in particular), it should contribute to the services' overall appeal rather than diminishing it. Nonetheless, this initiative will rely on industry willingness, and on evidence that this is something audiences really want.

Age verification

Age verification has two distinct forms: schemes intended to create secure identities for children to manage access to, for example, child-targeted fora and messaging services; and those intended to verify adulthood, as a means of preventing children from accessing potentially harmful content. In this context we are concerned with the second type of age verification – that used to control access to adult content.

Age verification is a tool that promises to be useful in controlling children's access to adult (harmful) content, but which in practice faces very significant challenges. There are three main reasons for this: the near-impossibility of truly secure verification, the cost of good verification and jurisdictional limits.

Firstly, it is very difficult to confirm age securely without some physical link between the website operator and the individual. For this reason, the German age verification process, giving access to regulated providers of pornography, involves visiting a Post Office or the use of a live webcam do demonstrate identity, or the physical receipt of a personal ID USB-chip. Without such measures, it is possible to refer to publicly available identity data, such as electoral rolls; or to use credit card numbers. However, all these measures are subject to significant leakage. In particular, while credit cards are unavailable to minors, debit and pre-paid cards are available to, and used by, those under 18.

In its analysis of the Child Online Privacy Protection Act, the US Federal Trade Commission noted that "current technology does not provide a practical means to prevent determined children from falsifying their age online… age verification technologies have not kept pace with other developments"[44]

44 http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf. Quotation is part of FTC report of public comments, but context makes clear their agreement

Even though such measures can contribute to the control of harmful content, they tend to be expensive, both for the individuals concerned and/or for the content provider using the service. For example, online safety expert Parry Aftab of Wired Safety noted that "The cost of obtaining verifiable parental consent for interactive communications is very high, estimated at more than $45 per child"[45].

Finally, age verification is inevitably limited by the reach of a national scheme: pornography providers to Germans must operate with the age verification process described above, unless they operate from anywhere outside Germany. Anecdotally, the introduction of this regulatory requirement resulted in a significant majority of German pornography providers moving their operations out of the country.

Given these issues, pursuing 'secure' age verification access to harmful content is almost without doubt a very challenging task. Nonetheless, the use of credit card data and other lower-cost means to verify age can help control the availability of potentially harmful content.

Option for consideration:

Although **age verification** has the potential to be valuable in managing risks to children, practical hurdles, including implementation and cost, will tend to limit its impact. Nonetheless, Ofcom recommends that the Byron Review team considers whether there might be any opportunity to encourage the use of age verification to restrict access to harmful content.

Age *confirmation*

The form of age verification used on many websites which feature potentially harmful content - including UGC, social networking and a significant proportion of US-based pornography sites - are essentially insecure. These sites simply require that users enter their date of birth, with no external verification of the users' claim. They will not prevent children who are seeking harmful content from finding it. However, children who are aware of the reasons these tools are in place can nonetheless use them to manage their content experience and avoid harmful content. Strictly speaking, this is more in the nature of a content classification and labelling initiative, than age *verification.* A set of content is classified as inappropriate for children, and children can use an age *confirmation* tool of this type to avoid exposure to such content.

Option for consideration:

The Byron Review team should encourage the use of such age *confirmation* tools by all providers of potentially harmful content, even though they are insecure.

To be effective this would also require parents and children to be aware of the valuable role that such age *confirmation* tools can play in helping prevent exposure to inappropriate or harmful content, and for parents to ensure that children make use of them. This should be a part of the general media literacy programme discussed earlier.

45 Parry Aftab, Filing in COPPA Rule Review 2005, June 27, 2005, p. 2 www.ftc.gov/os/comments/COPPArulereview/516296-00021.pdf Relates to verification of children's age, but cost issues are also material in relation to adults

Advertising content controls

Content which is made freely available online relies on advertising funding. Many of the institutions responsible for placing advertising make significant efforts to ensure that advertising, and the associated revenue, is channelled to appropriate content sites. It is not possible to determine the extent to which advertising revenue is unwittingly directed to harmful content providers. Nonetheless, the current systems are not perfect, as a result of a number of factors:

- Some industry sources have suggested that there is insufficient awareness among advertisers and agencies of the potential for advertisements and money to flow through to potentially harmful or inappropriate content sites.

- Some advertisers are indifferent as to the contexts in which their advertising is placed, though these are typically marginal brands, and account for a limited proportion of the total banner market.

- Management of the networks through which advertising reaches sites is a complex task. Network and affiliate network operators and providers are not always able to maintain complete control over the portfolios of sites to which their content flows, despite continued investment. Mainstream operators are, however, strongly incentivised to do so by the damage to their businesses caused when problems emerge.

- In the UK, the Internet Advertising Sales House (IASH) code of practice defines types of websites prohibited for its members' adverts, such as those featuring guns or obscene content, as well as websites where IASH members need to seek permission from the client before placing an advert, such as adult content or P2P sites. However, IASH membership currently excludes some of the leading advertising network operators. The reasons for this are hard to discern, although they do not appear to result from the lack of desire by network operators to provide controlled placement of advertising.

Option for consideration

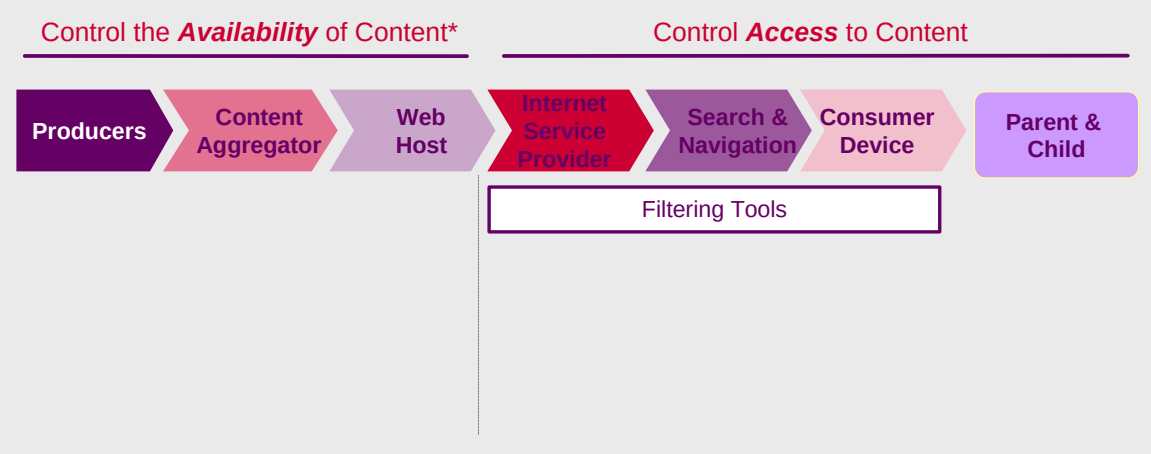
We recommend the Byron Review team considers exploring with the **online advertising industry** ways to reduce further the extent to which mainstream UK online advertising is placed around harmful content. Initiatives might include:

- encouraging greater take up of the IASH Code (or a similar framework) so that it covers a much greater proportion of UK online advertising sales; and
- information/education initiatives directed at improving awareness among advertisers and agencies of the means by which online advertising can be made more secure.

Controlling accessibility

There is a single technical means of controlling individuals' access to content: through the use of content filtering tools. A full description of filtering is included in Annex 2; in brief, however, content filters provide managed access to the internet by classifying content, and enabling different classes of content to be blocked.

Figure 20 The internet value chain: controlling access to content



Typical classification categories include: sexual activity, nudity, violence, drug use and gambling.

The threshold of acceptability or harmfulness for content varies according to the ages of children and their families' cultural backgrounds. To reflect this, filtering solutions are designed to be flexible and enable specific control of the types of content that should be blocked. Many filtering tools allow control on the basis of child age ranges, rather than in relation to the specific categories of potentially harmful content. For example, AOL's parental control tool distinguishes between three child categories - under-12s; young teens (13-15); and mature teen (16-17).

There is a wide variety of filtering tools available, and they are becoming increasingly sophisticated. In principle, it should be possible for internet filtering tools to play a key role in resolving the concerns of parents over the risks of harmful content. However, the use of filtering tools in the UK is partial: around half of all parents use filters to manage their children's internet access. To the extent that filtering seems to promise significant benefits, we must consider what hurdles exist to their wider adoption by parents.

Firstly, filters require parents to install and configure them. Although the providers of such software have an incentive to make the filtering products easy to use, it is still often a complex task. Among other things, parents who have children of different ages are required to create and configure distinct identities on a home PC, in order that both older and younger children have the right controls in place.

Despite the improvements in the sophistication of filtering products, they are perhaps most effective for younger children. For the youngest children – perhaps under 6 – the simplest 'pass list' filter may be appropriate. This will restrict access other than to a defined shortlist of child-appropriate websites – so there is no risk of under-blocking; and the fact that children will be unable to access a broad range of content which might be appropriate for them is arguably a lesser concern.

For older children, filtering tools typically rely on a combination of a blocking list - a defined of undesirable sites - and automatic decision-making about unclassified sites, using keywords, phrases and other indicators such as the type of language in use and the text-to-image ratio, and any available content labels and metadata. Although such tools are all subject to a degree of over- and under-blocking, an EU testing project in 2006 found that "filtering tools are generally capable of filtering potentially harmful content without seriously degrading the Internet experience of the youngsters". However, as children approach and enter their teens, they are increasingly likely to encounter blocked content which they wish to access, and which in some instances may be appropriate. In practice, parents of older children may face repeated requests that filters be removed in order to access specific pieces of content.

Finally, as has been demonstrated by the experience of the Australian Government in relation to its publicly-funded, freely available filtering products, teenagers are often very sophisticated computer users – with competencies well beyond those of most parents. Shortly after the free filtering software packages were released in Australia, there were widely reported stories of teenage experts breaking the filter; and once a tool has been cracked the relevant techniques quickly become available to all interested users. Although there will continue to be advances in the security of such products, this threat will limit the usefulness of filtering products for older children.

Nonetheless, filtering products are an essential tool in managing access to harmful content, particularly for younger children. The question is how to encourage their more widespread adoption.

ISPs and filtering

The leading consumer ISPs, which account for over 90% of UK internet subscriptions, all offer filtering products as part of their internet access proposition; and the majority of UK broadband subscriptions come with a free filtering solution. However, the provision of information about filtering, and support for parents in their use of the tools provided, does not appear to be as effective as it might be. Although ISPs do invest in filtering tools, and in support, the incentives they face are somewhat mixed: a message that internet access presents a significant risk of harm is not easily reconciled with the effective marketing of internet access.

More generally, the dominant characteristics on which internet access is marketed are bandwidth and price: value-added characteristics such as filtering or security support are used less to distinguish between service providers. For example AOL's internet access business, a core element of whose consumer proposition earlier in the decade was the promise of parental control, was sold to Carphone Warehouse in 2007. Although the AOL access proposition still includes parental controls, the current marketing communications focus on price and speed – with some packages also including the offer of a free laptop.

Option for consideration

We recommend that the Byron team considers exploring with ISPs and ISPA, their trade association, the development of a code of practice for family-friendly internet access, with relevant characteristics including the provisions of tools, information and support – for example in relation to parental controls for content filtering, and internet security (firewalls, spam-blocking tools). This code might also create a 'trustmark' or brand for family-friendly services, like those developed in France and Australia by ISPs and service providers.

Information and awareness initiatives could improve parental awareness of the potential benefits of such services and of the trustmark. This could help to create incentives for interested ISPs to focus greater attention on creating differentiated family-friendly access propositions.

Filter usability and relevance

In a number of other countries, there have been national schemes to encourage the adoption of filtering; along with information or educational initiatives, there are programmes to test filtering products for features including general usability, over- and under-blocking, presence of age-based filtering and content-category based options. In the UK, Ofcom has been working with the Home Office and industry to develop a BSI standard for filtering products, which will allow qualifying products to carry a Kitemark.

Option for consideration

Alongside other media literacy initiatives, we recommend that the Byron team considers promoting awareness of Kitemarked filtering products' benefits, and encouraging their wider adoption.

Filtering and complaints

One concern widely expressed about commercial filtering products is that they are relatively undifferentiated across countries: certainly the market for English-language products is dominated by US providers, which will mean that blocking and pass lists may fail to take account of specific UK cultural concerns; or of valuable or harmful local content.

In order to address such concerns, a number of regions operate a centralised register of illegal content, to be used by filtering and blocking tools. The most widespread form of this is the creation of blocking lists: for example, the UK and Sweden have centrally maintained lists of sites featuring child abuse images, which are used (voluntarily) by ISPs to block access. These lists are complaints-led: consumers who find potentially illegal content report their concerns, and after professional review illegal sites are added to the list. In Australia, the AMCA runs a similar scheme with a slightly broader remit – it includes child pornography; bestiality; excessive violence or sexual violence; detailed instruction in crime, violence or drug use; and/or material that advocates the doing of a terrorist act. The blocking list is incorporated into the range of Government-approved filtering solutions.

Similarly, the network-layer blocking systems operated in Saudi Arabia refer to a list run by the Communications and Information Technology Commission – which is open to online complaints, both about illegal content or about blocked sites which users believe should be made available.

The creation of a centralised register of potentially harmful content would be a Sisyphean task – the resources required to develop a list sufficiently comprehensive to have impact would be considerable, and would inevitably trail behind the proliferating availability of such material. However, UK internet audiences represent a valuable resource, whose contribution could help with the development of more effective UK-centric filtering products.

Option for consideration

As well as promoting the use of filtering products, we recommend that the Byron team considers ways of encouraging parents to be active users of such products, reporting instances of under- and over-blocking to their software providers. Over time, this information will help the development of products which better reflect the specific concerns and content standards of UK parents

Network and local filtering

Content filters can be applied at two points: at the network layer, by the ISP; and on the consumer device – the PC. In the UK, and in most of the rest of the world, consumer filtering is used at the PC rather than at the network layer, although the AOL internet access service incorporates network layer filtering.

One policy response to the limited adoption of filtering products by parents in the home, and given the issues identified above, is to propose the introduction of network layer filtering. However, this proposal does not offer significant advantages over filtering on consumer PCs – and raises some significant additional problems.

Firstly, the same practical hurdles exist in relation to network filtering as to PC filtering – parents would still need to configure the filtering software to reflect their specific concerns and the different ages of their children. Furthermore, enabling discrete filtering options would, for most ISPs, entail a very significant investment in enabling multiple identities at the ISP for those families who wished to have filtered and unfiltered access. Finally, network-layer filtering places material costs on ISPs, and can lead to problems with network performance and connection speeds[46].

For these reasons, outside states which have strong centralised policies in relation to the management of internet content, like China and Saudi Arabia, there has been very limited consideration of network layer filtering. In Australia, where plans to implement free network-layer filtering were announced by the Government in 2006, network layer filtering currently plays a limited role. An initial feasibility study carried out in 2006 found that network layer controls reduced performance significantly, especially for larger ISPs. The approach may nonetheless be implemented, following feasibility research and input from a trial of ISP filtering currently taking place in Tasmania, but future developments remain uncertain.

Mobile internet access and filtering

The use of mobile devices to access internet content presents some additional challenges and opportunities for the management of harmful content risks. The challenges emerge because the market for filtering solutions which can be installed and run locally on mobile devices is undeveloped, and mobile phones are used by children without parental supervision.

However, mobile networks and devices are, at least at present, a much more appropriate platform for network filtering: the devices are owned by individuals, so complex configuration for multiple users is not necessary; the range of services accessed is narrower; and the volume of internet data traffic is much lower than for fixed internet connectivity.

[46] Please see results of a feasibility study in Australia in 2006.

In the UK all the mobile network operators comply with a joint industry code of practice which requires access controls for the operators' own content portals; and requires that they offer network-layer filtering for the internet. For both of these services, the account-holder can specify whether or not the phone should allow access to content for adults (18-rated content). No comprehensive evidence exists as to the levels of application and effectiveness of this code of practice. Ofcom, in partnership with the Home Office and the Children's Charities Coalition on Internet Safety, have begun an audit which will result in the publication of a review with recommendations in 2008.

In France, at least one network operator has committed to providing a further level of support for parents: as well as offering the under-18 class of network filtering, they propose to allow parents to also specify a 'child profile' (under 12), further limiting the range of content accessible.

Options for consideration

We recommend that the Byron Review considers encouraging the mobile network operators to extend their commitment to network filtering, and allowing parents to specify a child-friendly filtering option analogous to that possible within most PC filtering tools.

Glossary of terms

ACMA	Australian Communications and Media Authority, the Australian converged communications regulator
AVMS	Audiovisual Media Services Directive: new EU Directive covering the regulation of linear and on-demand television
BBC	British Broadcasting Corporation
BBFC	British Board of Film Classification, responsible for the provision of age-ratings for films and some video games
BECTA	British Educational Communications and Technology Agency: leads the national drive to improve learning through technology and supports the education sector to make the best use of technology
BFI	British Film Institute
CEOP	Child Exploitation and Online Protection Centre: works across the UK and maximises international links to tackle child sex abuse
FTC	Federal Trade Commission, the US competition regulator
Host	Term used to refer to a computer connected to a network such as the Internet
Hosting	Storage of content and applications on servers connected to the Internet
IASH	Industry body representing Internet Advertising Sales Houses
ICANN	Internet Corporation for Assigned Names and Numbers has overall responsibility for managing the DNS
ICRA	ICRA is part of the Family Online Safety Institute, an international, non-profit organization of internet leaders working to develop a safer internetInternet. Responsible for the ICRA content labelling and classification framework
IP	Internet Protocol. The packet data protocol used for routing and carriage of messages across the Internet and similar networks
IPPR	Institute for Public Policy Research: UK policy thinktank
ISP	Internet Service Provider. A company that provides access to the Internet
ISPA	Internet Service Providers Association, UK trade association responsible for co-ordinating the ISP industry
IWF	Internet Watch Foundation, a UK based organisation which seeks to rid the Internet of illegal material such as child pornography
Peer-to-Peer (P2P)	A method of communication in which two hosts or applications can initiate communications with each other and share resources