Ofcom Report on Internet safety measures

Strategies of parental protection for children online

date: 15 January 2014

Contents

Section 1

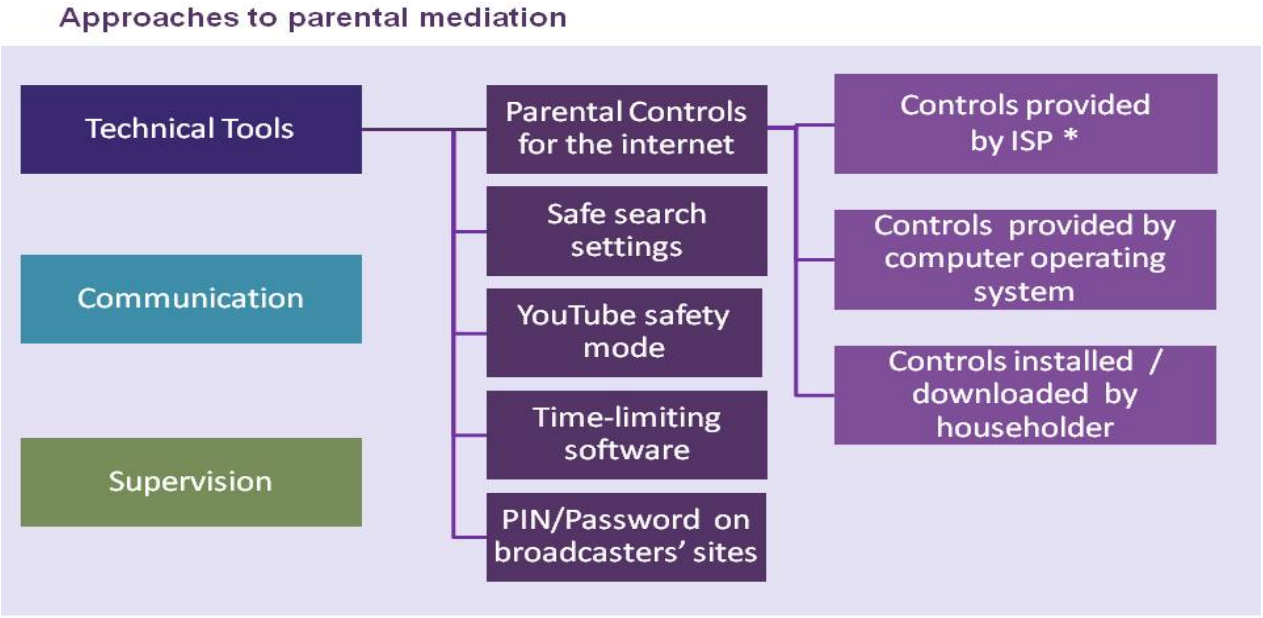
Executive Summary

1.1 Ofcom welcomes the opportunity to report on its media literacy research regarding parental mediation of the internet and the wide ranging strategies and tools used by parents to protect their children online. This report is the first of three which will be provided in response to a request from the Department of Culture, Media and Sport ("DCMS") following Government requests to UK Internet Service Providers ("ISPs") regarding implementation of network level filters[1].

1.2 DCMS requested that Ofcom report on the take-up, awareness of and confidence of parents in relation to parental controls, including:

- the broader strategies parents may adopt to improve children's online safety;
- the levels of parental awareness and confidence with the safety measures which may be in place on sites regularly visited by children including, but not restricted to, content providers, search engines and social networking sites; and
- any research into why parents may choose not to apply technical parental control tools.

1.3 Parents use a range of strategies from communication and supervision (including social media monitoring), to the use of technical controls to manage their children's access to the internet.



* ISP-provided controls could include: network level filtering e.g. 'Homesafe' from TalkTalk or software - like McAfee Family Protection - provided by ISPs for people to install on their computers.

[1] Full details of the request can be found at Annex 1.

1.4 As illustrated above there are a range of technical tools that parents employ including:

- Parental controls offered by the ISP[2];
- Parental controls offered by the computer's operating system; or
- Parental controls through programmes installed or downloaded by someone in the household.

These three types of technical control are referred to collectively in the research data as "Parental controls" but the research also covers:

- Browser based controls like Safe Search;
- Time limiting software;
- YouTube Safety Mode; and
- Content provider guidance such as Pin protected content.

1.5 The report also provides a contextual explanation of the chain of supply in which these tools operate and explains how they are positioned in the context of the broader parental mediation strategies of discussion, rules and monitoring - which for the majority of parents are a crucial part of how they manage the risks to their children online.

1.6 Aspects of the regulatory framework for online content are set out at Annexes 2 and 3. Annex 2 sets out the regulatory framework relating to Ofcom's powers and duties in relation to some online content. Annex 3 turns to the provisions of the E-commerce directive regarding intermediaries (further explained in section 4) but we recognise that beyond this framework lie the challenges created by the nature of the open internet.

The context: parenting in an internet age

1.7 Parenting in the digital age, against a backdrop of continuing technical evolution, can be complex and challenging as children rapidly take up the opportunities of internet use. According to our research use of tablets has tripled this year, becoming the device of choice for 8-11s to access audio visual content and games in particular. Over six in ten 12-15s now own a smartphone and it is the most popular device for social networking among that age group.

1.8 Children's confident adoption of new technologies has many positive outcomes with benefits of use ranging from education, communication, social engagement and entertainment. But there are also perceived risks, particularly around internet **content**, and the **conduct** and **contact** risks inherent in peer to peer communication facilitated by the internet. Although the vast majority of children say that they are confident they can stay safe online the research also shows their levels of confidence have fallen slightly from previous years. The research notes some trends around

[2] ISP-provided controls could include any of the following: network level filtering e.g. 'Homesafe' from TalkTalk or software - like McAfee Family Protection - provided by ISPs for people to install on their computers.

unsafe behaviours, such as maintaining an open social network profile[3], and indicating that children are less likely to know how to block online messages from people they don't want to hear from.

Parental concerns

1.9 The vast majority of parents say they trust their children to use the internet safely. This agreement increases with each age-group, consisting of 52% of parents of 3-4s, 72% of parents of 5-7s, 83% of parents of 8-11s and 89% of parents of 12-15s. However, parents also report having concerns about their child's online activities. Parental concerns tend to be higher around issues identified in this report as relating to contact and conduct with around one quarter of parents concerned around cyberbullying and a similar number concerned about downloading bogus applications and viruses. One in five parents are concerned about who their child is in contact with and the risk of the child giving out personal information to inappropriate people. Around one sixth of parents are concerned about the issues identified in this report as content issues which their child might encounter online.

1.10 That said, the vast majority of parents feel that the benefits of the internet outweigh the risks and around half feel they know enough to help their children stay safe online. Overall, half of parents of 5-15s agree that their child knows more about the internet than they do but this also varies by the age of the child – from 14% of parents of 3-4s up to 63% of parents of 12-15s.

Main conclusions of the report

Parental strategies are a combination of mediation and controls

1.11 The quantitative findings from the 2013 Children and Parents: Media use and attitudes report[4] study showed that the vast majority of parents are actively engaged in mediating their child's online activity in some way. Most use a combination of approaches including:

- Regularly talking to their children about staying safe online. Almost eight in ten parents say they have talked to their child about online safety with 45% doing so at least monthly.
- Having rules relating to parental supervision. Over half of parents have set rules around supervision of the internet which include regularly checking what children are doing online or only using when supervised.
- Mediation through technical tools. Over six in ten parents use some kind of technical mediation such as parental controls, safe search settings, You Tube safety Mode, time-limiting software or PIN/Passwords set on broadcaster's websites.

1.12 Overall, 85% of parents with a child that goes online at home via a PC/laptop or netbook use at least one of these approaches with 20% using all three, 35% using two and 30% using only one. Fifteen per cent of parents use none of these mediation techniques.

[3] One third of 12-15s with a social networking profile in 2013 have it set so that it can be potentially viewed by people unknown to them. This is up from 22% last year.
[4] http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/october-2013/research07Oct2013.pdf

1.13 A 2012 qualitative study into parents' views on parental controls[5] suggested that the approach parents took to mediating the potential risks to their children in the online sphere was generally consistent with their overall parenting style. Respondents typically spoke of their aim to balance rules and boundaries with trust and freedom. Instilling the right values and habits in their children was seen to be critical.

Parents' use of a range of technical tools and other safety measures on sites regularly used by children

1.14 However, as paragraph 1.09 indicates, technical tools also play a part in many parents' online parenting strategies with six in ten parents of children who use a PC/laptop/netbook to go online at home using some form of technical mediation. These include:

- 43% of parents of online 5-15s and 40% of parents of 3-4s report having parental controls as defined above[6] in place on a PC, laptop or netbook. A majority of parents with parental controls set on their device agree strongly that these controls are effective and that their child is safer as a result.
- Safe search setting: Four in ten parents of online 5-15s say they use safe search settings on search engine websites.
- Time-limiting software: One in ten have software installed to limit the amount of time a child can spend online.
- YouTube Safety Mode: Two in ten parents have the Safety Mode set. This increases to three in ten parents of children who actually visit the YouTube website through a PC/laptop or netbook.
- Content provider guidance: One in three online children now watch television content via UK television broadcasters' websites. Around one in four of the parents who are aware of the guidance labels have set up a PIN or password to be used before viewing programmes that have a guidance label (24% of the 67% aware of guidance labels).

1.15 Social media monitoring also plays a role, with parental awareness of the minimum age requirement for Facebook having increased among parents whose child has a profile on this site and 73% of parents check their child's social networking site activity. In addition, figures from the 2012 study[7] shows that where the parent and the child have a profile on the same website, 97% are 'friends'.

Non take-up

1.16 Over half of parents do not use parental controls in the form defined by this report, i.e. those provided by their ISP[8], their computer's operating system or programmes installed or downloaded by someone in their household.

[5] http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2012/Annex_1.pdf
[6] Parental controls in this report means either provided by the ISP, provided by the computer's operating system or programmes installed or downloaded by someone in the household.
[7] http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2012/main.pdf
[8] ISP-provided controls could include any of the following: network level filtering e.g. 'Homesafe' from TalkTalk or software - like McAfee Family Protection - provided by ISPs for people to install on their computers.

1.17 The main reasons for non take-up of parental controls, as identified in the 2013 quantitative survey, are a combination of trusting and supervising the child – depending on the age of the child.

1.18 The 2012 qualitative study also showed that a lack of awareness and understanding of parental controls appeared to be a key reason for non-take up. The study suggests that there is a perception, particularly amongst parents with lower levels of confidence about technology, that the process of selecting and installing parental controls was complex and time-consuming.

1.19 The qualitative findings also suggested the potential value of parental controls did not appear to be front-of-mind on a daily basis for parents. In the absence of a specific trigger many parents without parental controls admitted 'not getting around' to considering them. Their reported focus was more on the issues and problems that they were regularly experiencing with their children's day-to-day internet use (e.g. children spending too much time online) rather than around the risks which few parents had any direct experience of (e.g. of physical and psychological harm related to exposure).

1.20 In addition, even amongst those who had installed parental controls, many had not given them much further thought and protections may have become outdated as a result of this lack of continuing engagement.

1.21 Overall, parental controls were viewed as a supplement to, rather than replacement for, hands-on parenting. Supervision and other forms of parental mediation were felt still to be needed to manage all of the day-to-day issues their children faced, including risks emanating from children's internet usage.

Structure of this report

Following the Executive Summary in section 1 the report has a two-part structure as follows:

Part 1 The Context of the Internet

Section 2 – Opportunities, risks and challenges
Takes an overview of children's access to the open internet as an educational resource, as a platform for communication and creativity, but also as a source of distinct risks around content, contact and conduct, with specific regulatory challenges.

Section 3 - Parental mediation: managing the risks to children
Describes the tactics of parents, carers and educators in guiding and informing children's behaviour through education and advice, mediation and rules as critical aspects of child protection online.

Section 4 - Safety mechanisms and the role of industry
Describes in detail many of the tools and mechanisms offered to parents to protect their children online and notes some of the issues around such tools. It does so within a simplified model of the internet from content origination to content reception by the user and gives an overview of the status of internet intermediaries like ISPs.

Part 2 The Research

Section 5 – Children and the internet: use and concerns
Sets the context for mediation by looking at key changes in children's use of the internet, their likes and dislikes compared to the online concerns of parents.

Section 6 - Parental mediation strategies: take -up, awareness of and confidence of parents in relation to parental controls
Provides both quantitative figures and qualitative insights to create an in-depth picture of the broad range of online mediation strategies employed by parents and their levels of confidence about their ability to keep their children safe online.

Section 7 - Safety measures on sites regularly visited by children
Looks at the research available regarding parental mediation of websites regularly visited by children, including search engines, YouTube and social networking sites.

Section 8 - Why parents choose not to apply parental control tools
Looks at the various reasons why some parents choose not to install parental controls.

Section 2

Part 1 The Context of the Internet

Opportunities, risks and challenges

2.1 Children are active and enthusiastic participants in the online world with 81% of 5-15s accessing the internet at home and increasing to 97% for 12-15s[9]. The recent Oxford Internet Surveys ("OxIS") report "*Cultures of the Internet: The Internet in Britain 2013*" found that households with children are by far the most likely to have internet access (95% of homes with a 10-17 year old have access, against 75% of homes without children)[10].

2.2 This report recognises that, alongside the risks that the tools examined in this report seek to mitigate, there are benefits of access to the internet for children in a broad range of ways. The internet as an educational resource, as a platform for social interaction and creativity and as a source of entertainment are part of the landscape parents negotiate when considering responses to those risks.

The opportunities for children presented by the internet

Education and skills

2.3 Internet use is recognised to be an important skill in its own right for children, in addition to its use as an educational information resource. Competence in internet use is a target of all the national curricula in the UK, for example the English National Curriculum states that children from Key Stage 1 are expected "*to be able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world*"[11]. By Key Stage 2 children are expected "*to understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration and to be able to use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content*".

2.4 The educational benefits of the internet are well appreciated by parents. Research conducted by Ofcom indicated that parents see the internet as an invaluable homework and learning resource for their children; they also felt that gaining proficiency in using the internet would be critical to their children's future prospects:

> "*They definitely have more knowledge than when we were at that age…It's amazing and I think it's all because of the internet and TV and modern*

[9] http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/october-2013/research07Oct2013.pdf.
[10] OxIS "Cultures of the Internet: The Internet in Britain 2013" Dutton, Blank and Groselj p52. http://oxis.oii.ox.ac.uk/sites/oxis.oii.ox.ac.uk/files/content/files/publications/OxIS_2013.pdf
[11] The National Curriculum in England: Key stages 1 and 2 framework document ps 178 – 179 https://www.gov.uk/government/publications/national-curriculum-in-england-primary-curriculum

communications…At school their homework is determined by the computer. They've got to do it online and they have their own email address at the school"[12].

Communication and social interaction

2.5 The internet offers a broad range of opportunities for communication, including one-to-one and as part of broader social environments, for example on social networking sites. Children use the internet, and in particular social network sites, as a way of connecting with peers: quantitative findings from our 2013 survey show that 68% of 12-15s had set up a social networking profile and the average estimated number of friends they had on social networking sites was 272.

2.6 Internet communication may be especially advantageous for shy or socially marginalized children, enabling them to practice social skills without the risks associated with face-to-face interactions. Adolescents may share thoughts and feelings online more easily than they would in person, building confidence in managing real social situations[13].

Creativity and entertainment

2.7 Whilst children's media use remains dominated by TV, the forms of entertainment and cultural engagement available online are myriad, and children's enjoyment of these as consumers, and as innovative creators of content, comes a close second to its use as an educational tool[14].

2.8 Tools for producing and circulating different kinds of content – text, images and videos – are widely available and affordable to many people, including children, around the world. A child can record a video on their smartphone and share it with a global audience of more than two billion users[15]. Safe access to "the dizzying potential of digital technology"[16] to transform the way children receive and exchange ideas about arts and entertainment is an exciting benefit of internet use, but the very nature of that dizzying potential creates risks to children using the internet. We have grouped these in broad terms below.

The risks of harm to children online

Potentially harmful content

2.9 Internet content originates from anywhere in the world and is offered everywhere in the world. Publishing online, using simple technologies and software is now possible for a wide range of people previously barred from content creation by costs or technology.

---

[12] Report prepared for Ofcom by Jigsaw research: "Parents' views on parental controls: Findings of qualitative research".http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2012/Annex_1.pdf

[13] See for example "Adolescents and the Internet" Nathalie Louge, Cornell, 2006, and "Relationship formation on the Internet: What's the big attraction?" McKenna, Green, and Gleason. Journal of Social Issues, 58, 9-31 2002. and "Adolescents on the net: Internet use and well being": Subrahmanyam and Linht 2007.

[14] Source: "EU Kids Online: National perspectives" Haddon, Livingstone and the EU Kids Online network – 83% of 9-16 year olds use the internet for playing games and 76% for watching video clips compared to 86% for educational use.

[15] Http://www.internetworldstats.com/stats.htm

[16] Sector Skills Assessment for the Creative Media Industries in the UK, Skillset, 2011, p14.

2.10 Whilst this freedom creates possibilities of expression and communication, new content providers may be indifferent to or ignorant of the kinds of rules and controls which their own territories adhere to and many will be unaware of international cultural sensibilities. This may be particularly acute amongst the non-professional "user generated content" providers, despite the increasing sophistication of personal contributions to content online found throughout the internet in blogs and YouTube channels. The consequence of these factors is that children using the internet may risk exposure to content which may pose a risk of harm – for example in the form of sexually explicit content.

Potentially harmful contact

2.11 The internet also enables many forms of communication allowing contact with individuals known and unknown, from direct one-to-one communications such as email and instant messenger, to one-to-many forms such as posting content, status updates and recommendations (liking) on social networking sites. Such information-sharing may also reveal details of an individual's lifestyle, preferences and location. All of these forms of contact may expose children to harm, either as recipients of abusive messages (victims of cyberbullying) or in allowing them to communicate or share information with unknown individuals, including adults who may seek to harm them (online grooming).

Potentially harmful conduct

2.12 These communication and publishing opportunities also create the possibility that children's own conduct online can create risks for themselves and their peers, for example by originating or distributing potentially harmful or abusive content; failing to safeguard personal content from unknown individuals; and/or ignoring the risks to their safety on and offline created by widespread distribution of their personal information.

The challenges of regulation

2.13 The internet was created through international cooperation and is designed for global access to information. It is as distinct from the type of local analogue content that television represents as television itself was from the printing press. This step change in the nature of the content delivery mechanism, the internet and the interlinked pattern of benefits and risks laid out above increases the complexity faced by parents seeking to control their children's exposure to potentially harmful material.

2.14 The particular challenges the open nature of the internet poses to parents seeking to mediate their children's online experiences include:

- **The global nature of online content distribution**. The international nature of content provision and the global nature of the players within the provision of the architecture of the internet not only provides challenging cultural differences in content, as noted above, but strongly affects effective national regulation.

- The UK has long sought to restrict access for children to some types of content which it considers may be harmful to children, even though adults may legally acquire it. The regulation described in Annex 2 does cover certain forms of online content distribution through Video-on-Demand services, where services are based in the UK. However, whilst it can be easily accessed in the UK, as much of the content on the internet derives from international sources, it largely falls outside this regulation.

- **Diverse and ubiquitous internet access.** The internet is accessible almost everywhere – at home, school, in internet cafés and anywhere there is access to wifi or mobile broadband; and is mobile too, on a wide range of devices, including tablets and smartphones. Potentially harmful content is available online constantly rather than during defined time periods as is the case with broadcast television. The traditional regulatory mechanisms of restricting children's access either physically – by barring under 18s from sex shops selling R18 sexual material – or temporally – with the watershed providing an effective child protection mechanism in relation to the television in living rooms – do not work for the internet. New methods, based on the nature of electronic communication, must be found.

Section 3

Parental mediation: managing the risks to children

3.1 Given the risks and challenges described above, the actions of parents, carers and educators in guiding and informing children's behaviour are a critical aspect of child protection online, alongside the contributions played by service providers in offering mechanisms and tools to enhance child safety.

3.2 The importance of parental support, guidance and information provision is acknowledged by virtually all participants in the debate about child online harms. For example, in evidence to a CMS Select Committee inquiry into online risks to children[17], Jim Gamble, then CEO of the Child Exploitation and Online Protection Centre (CEOP)[18] said parents have: "*a responsibility with regard to how you empower young people with information which makes them safe*".

3.3 Dr. Tanya Byron's 2007 report into harmful content online said that parents: "*...have a key role to play in managing children's access to [potentially harmful] material...restricting children's access to harmful and inappropriate material is not just a question of what industry can do to protect children (e.g. by developing better parental control software), but also of what parents can do to protect children (e.g. by setting up parental control software properly) and what children can do to protect themselves (e.g. by not giving out their contact details online)*"[19].

3.4 More recently, Reg Bailey's 2011 report into the sexualisation of childhood said "*For us to let children be children, we need parents to be parents. Parents are clear that they have the main responsibility to raise their children, and to help them deal with the pressures of growing up*"[20].

3.5 Giving evidence to the CMS Select Committee inquiry into children's online safety, in October 2013, Anthony Smythe, Managing Director of the charity Beatbullying said "*the most useful parental control is parental responsibility*"; at the same session Claire Lilley from the NSPCC said "*We need to give parents confidence and empower them to think that they can deal with these issues, because the evidence does show work by Sonia Livingstone at the LSE – that when parents lay down boundaries and guidelines for their children, children will adhere to those. That is where the point comes in again about educating children about how to behave*"[21].

3.6 In outline, parents have four broad approaches they can adopt to secure their children's online safety:

---

[17] http://www.publications.parliament.uk/pa/cm200708/cmselect/cmcumeds/353/8031803.htm, question 167

[18] The Child Exploitation and Online Protection Centre (CEOP), the UK Police body is dedicated to eradicating the sexual abuse of children. CEOP tracks and seeks prosecution of offenders, such as those who create, distribute or consume child abuse images. This body works closely together with The Internet Watch Foundation (IWF) a self-regulatory regime funded by telecommunications and internet companies, which works to restrict the availability of child abuse images online.

[19] http://dera.ioe.ac.uk/7332/1/Final%20Report%20Bookmarked.pdf, p 5

[20] https://www.gov.uk/government/publications/letting-children-be-children-report-of-an-independent-review-of-the-commercialisation-and-sexualisation-of-childhood, p 11

[21] http://www.publications.parliament.uk/pa/cm201314/cmselect/cmcumeds/uc729-i/uc72901.htm, question 16

Education and advice: Parents can teach their children about the risks of harm, why certain types of online behaviour may expose them to harm and how to avoid doing so (e.g. discussing social networking privacy settings or how to handle contact from unknown individuals). Open discussion of the risks to which children may be exposed is particularly important, as it may help encourage children to let their parents know when they have unpleasant or distressing experiences (for example, if they are subject to abusive comments/bullying).

Supervision: Parents can directly supervise their children's internet use, the sites and services they visit and the interaction and communication in which they participate. Supervision is likely to be most relevant for younger children.

Rules about internet use: These may cover place and time: e.g. "only access the internet in the living room/when there is a parent present"; "only access the internet for x hours a day". Rules about online interaction and behaviour may help complement education and advice (e.g. "only communicate with friends/people you know").

We further detail parents' use of all of these types of mediation techniques in the research sections 6-9.

Tools and safety mechanisms: Finally, there are the technical tools we outline in the following section including filtering software and site safety mechanisms to restrict the internet sites and services to which children have access.

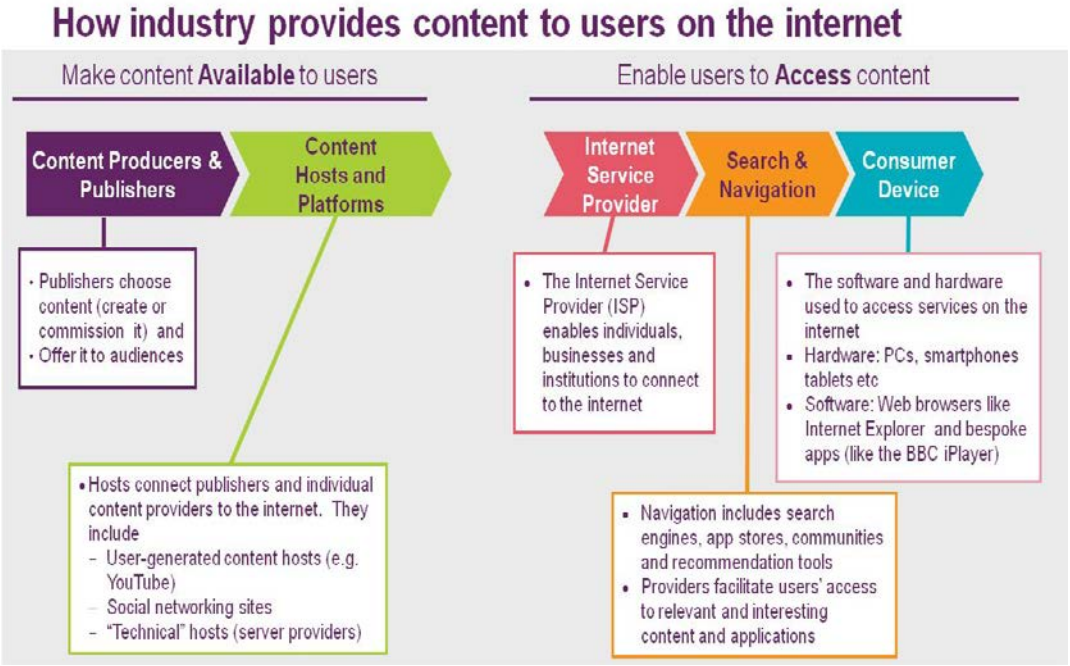
Section 4

Safety mechanisms and the role of industry

4.1 This section describes the various tools and mechanisms that different internet players can offer parents and children seeking to safeguard their online access and notes some of the issues around such tools. It does so within a model of the internet that describes some of the actors within the chain of supply from content origination to content reception by the user and gives an overview of the status of internet intermediaries like ISPs. The model is, for the sake of clarity, simplified and does not include some relevant players – such as advertisers and payment providers and the internet user communities – all of whom may have an influence on the editorial decisions taken by hosts and content providers.

A model of internet content provision

4.2 In order to explain the different types of safety mechanisms and tools, we have set out below a simplified model of the internet to explain the roles of certain key players involved in the creation and distribution of content over the internet. The framework comprises five segments, ascribed with a discrete function (see table below), although clearly those involved in internet service provision may operate in more than one segment.



Content producers and publishers

4.3 Content producers and publishers create or commission the content available on the internet. This category includes a wide range of professional and non-professional producers from content providers acting in several distribution formats from broadcast to online as well as online-specific content producers and individuals who upload user-generated content onto hosting sites like YouTube.

Hosts and platforms

4.4 In order for content to be available to audiences, it must be *hosted* – stored on a computer server which is connected to the internet. Content publishers and producers can make their content available on the internet in two primary ways:

- By paying for hosting services – either by running their own servers and contracting for their own connection to the internet; or by leasing a server or space on a server from a specialist provider, who will also provide a connection to the internet; or

- By posting or uploading their content to a "free" (advertising-funded) hosting website; for example a user-generated content site like YouTube; a blogging site like WordPress or a social networking site like Facebook.

4.5 The providers of hosting services have a special legal status as "hosts" under the E-Commerce Directive: they cannot be required in law to monitor the characteristics of the content they host, nor be held liable for hosting illegal content. Their protection from liability does, however, end when they are informed about illegal content: a host must then act to remove or delete the offending material. The role of hosts and the balance between their freedom from liability/obligations and the contribution which society may expect of them – for example in relation to child safety – is a central aspect of the debate about the responsibility of service providers in the online environment. More detail on the legal status of hosts can be found at Annex 3.

Internet service providers (ISPs)

4.6 ISPs provide internet access to individuals and organisations. ISPs either own the physical access facilities or procure them from an access provider. In order to connect to the internet, an ISP interconnects and exchanges traffic with other ISPs. Like hosts, ISPs have a special legal status: they are "mere conduits" and cannot be held responsible if their services are used to access illegal sites and services, or be required to monitor their users to identify illegality. More detail on the legal status of mere conduits can be found at Annex 3.

Search and navigation

4.7 Search engines and online communities facilitate users' access to content. Search engines allow users to search the internet using keywords. Online communities and social networking sites allow their users to share links to content which may be of common interest. Search engines are considered in some jurisdictions to have a "host" responsibility – and hence must remove from their search indices links to illegal content of which they are made aware. More detail on the legal status of hosts can be found at Annex 2.

Consumer devices

4.8 Consumer devices consist of the hardware and software that enable users to access content hosted on the internet. The device will interpret and present the content that arrives at the device into a form which is accessible by the consumer. Consumer devices such as PCs, tablets, smartphones and games consoles may use general internet browsers, such as Internet Explorer, to view web pages and bespoke applications providing access to a single service, like the BBC iPlayer or a Facebook application.

Internet management layer

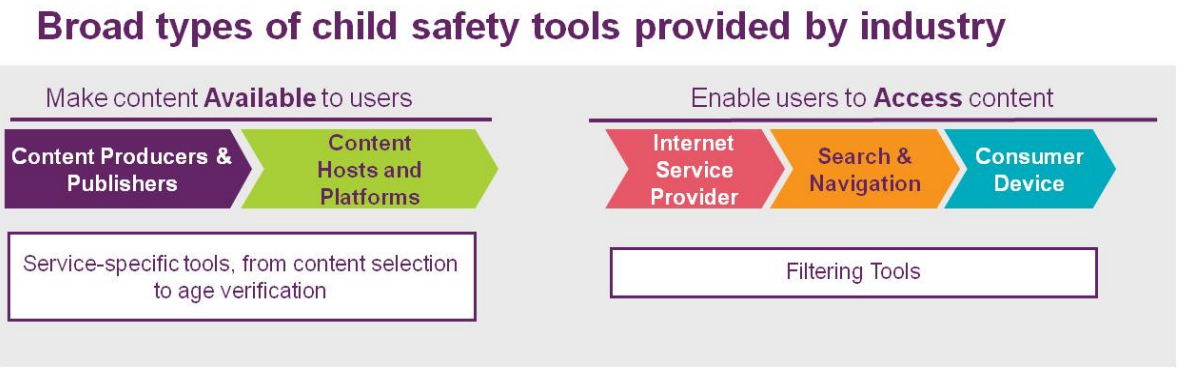
4.9 The internet management layer consists of the international, regional and national bodies which manage the technology and addressing system which underpins the internet. They ensure that the technology standards that support the internet, such as the internet language HTML and the transport protocol TCP, are interoperable. They enable consumers and producers to communicate through their *IP addresses* and the *domain name system*.

4.10 An *IP address* is intended to identify a device attached to the internet and hence to allow content and services to be routed between producers and consumers. There are some complexities in the operation of the addressing scheme which mean individual devices and individual websites can share IP addresses.

4.11 The *domain name system* translates between the domain names we use for sites and services – such as www.ofcom.org.uk – and the IP addresses of the computers where the sites or services are held.

4.12 Having established this model of five players – the content producers, content hosts and platforms, ISPs, search and navigation services and devices – we now turn to the specific tools they each can provide to parents.

The tools service providers contribute to children's online safety



4.13 Broadly speaking, there are two ways in which service providers can contribute to children's online safety:

- **Filtering**: The objective of a filtering system is to block access to websites and internet services which offer potentially harmful material. To be effective, a filtering solution must provide broad coverage of a child's internet use: filtering tools must be applied at a point of access – for example, on the child's device, or in the network by the internet access provider. (As we note below, it remains a very significant challenge for any filter – network or device-level – to deliver comprehensive coverage of online services).

- **Service-specific safety measures**: Individual service providers can offer tools which help parents protect children and help children protect themselves from harm. These tools and mechanisms range from age-verification of users, to restrict access to content inappropriate for children, through to the privacy settings on a social networking site, which may help protect children from contact with unknown adults. These tools are an essential complement to filtering/blocking, as there are many sites and services which include material for

children and also create risks of harm. For example, many parents would not wish to block access to the BBC iPlayer, even though it gives access to some content which is only appropriate for adults; similarly, many parents would wish to allow their (older) children to be able to use social networking sites to communicate and share content with their friends even though they may be exposed to potentially harmful contact.

Filtering tools to block access to potentially harmful content

4.14 The objective of a filtering system is to block access to websites and internet services which raise concern, and in this case may pose a risk of harm to children. It entails:

- Categorising content according to specific editorial criteria; and
- Restricting access to content in the desired categories.

4.15 Typical categories might include sexual activity; violence; drug-related content; gambling; alcohol; tobacco. (Many filtering providers also include a "proxy" or "anonymiser" category, intended to block access to sites/services which might otherwise be used to bypass filters; this is discussed further below).

Blocking lists, pass lists and labelling

4.16 Two types of lists are used by filtering tools:

- Blacklist (Prevent) A blocking list is used to identify the locations of potentially undesired content and consists of sets of web addresses (URLs), domain names e.g. example.com and server IP addresses. Blocking lists assign content assets to different categories according to their editorial characteristics. These may include age ratings or categories like *sexually explicit* or *violent*. This enables filtering systems to provide different levels of filtering appropriate to different age groups and cultural sensitivities;
- Whitelist (Allow) are the opposite of blocking lists – they list those locations where the content is known to be 'safe'. They are particularly useful for controlling the access of younger children who need a higher level of protection and are less likely to want to surf the internet in the same way as older children and adults.

4.17 List generation is a complex task, although user feedback and automatic tools can be used to help maintain and extend lists. Individual content assets on sites carrying rapidly-updated and/or user-generated content such as videos and photographs are in practice impossible to rate reliably using automatic tools though some providers may try to make use of text tags and labels attached to content; other filters address this concern by blocking such sites as a whole. Blocking systems may "crawl" uncategorised websites and attempt to perform automated analysis for automated categorisation. (Website crawling is a technique commonly used by search engines find new content).

4.18 The provision of accurate content labels or metadata by content providers would help filtering systems to categorise content correctly. However, only a tiny proportion of websites are labelled in a way that allows easy categorisation for the purposes of filtering.

4.19 There are some general concerns about the efficacy of filtering tools, as well as the specific advantages and disadvantages of filtering at different access points. The three general issues are:

- Underblocking and overblocking;
- Content which is outside the filtered environment;
- Children bypassing filters.

Underblocking and overblocking

4.20 All filtering systems are subject to a degree of overblocking (restricting access to acceptable content) and underblocking (permitting access to unacceptable content). There are a number of reasons for this including:

- The practical difficulty of accurate automatic classification;
- The scale of the internet, and the pace at which new content, sites and services are added;
- The misclassification of content;
- Differences in language and cultural focus – for example, some European content may not be identified or rated by US-based filtering software providers.

4.21 The EU Safer Internet Programme benchmarks filtering tools and services on a number of criteria; all of the tools tested over and underblock. The Safer Internet SIP-Bench report concludes broadly that users face an unavoidable trade-off between over and underblocking. "*Overblocking and underblocking rates are linked: tools with a low underblocking rate have a high overblocking rate*"[22] and vice-versa.

4.22 If an effective and transparent appeal or redress scheme for content suppliers whose content is blocked is integrated into the filtering operator's system, the harmful outcomes of overblocking may be somewhat reduced. Similarly an effective consumer reporting or complaints scheme for unblocked "harmful" content may also help address aspects of underblocking, but the problems of over and underblocking will remain given the scale and speed of growth of the content offered online and the consequent need to use automated categorisation tools.

Content which is outside the filtered environment

4.23 The primary focus of filtering tools is content on the World Wide Web, accessed using a web browser such as Internet Explorer, Chrome or Safari. (The World Wide Web is comprised of text, graphics, audio and video accessed using the HTTP protocol – it is most of what we think of as the internet, but not all). However, the web is not the only source of content; potentially harmful content is also widely available via newsgroups and peer-to-peer ("P2P") file-sharing networks. Content can also be exchanged via File Transfer Protocol ("FTP") technology, which allows you to transfer files between two computers over the Internet, instant messaging and email. Because of this, internet filtering systems typically may also offer options to manage

[22] Benchmarking of parental control tools for the online protection of children: SIP-Bench II Assessment results and methodology (5th Cycle) http://www.sipbench.eu/transfer/Report_5th_cycle.pdf.

access to these protocols and services. However, as tools like email, instant messaging and FTP may have both harmful and acceptable uses, filtering – in other words blocking all uses – is a less satisfactory means of controlling risk: parents may reasonably wish to allow their children to use messaging, email and other communications services.

4.24 The emergence of apps has created a new challenge, as app content, in most cases, is currently not controlled by standard filtering tools, which typically cover the World Wide Web. Unlike a browser, an app may not use the same network protocols as web browsing and therefore may not necessarily be subject to the network filtering system deployed by the ISP or be addressed by broader blocking, such as of P2P. The widespread use of smartphones and tablets by children (62% of children aged 12-15 have a smartphone and 23% of children aged 5-15 go online via a tablet) introduces a new task for parents who wish to control the content to which their children have access. Controlling apps requires an additional mechanism, which places restrictions on which apps can be installed on a device.

4.25 Parents therefore face some complex challenges in understanding the scope and effectiveness of the different types of filtering tools they might use

Children's ability to bypass filters

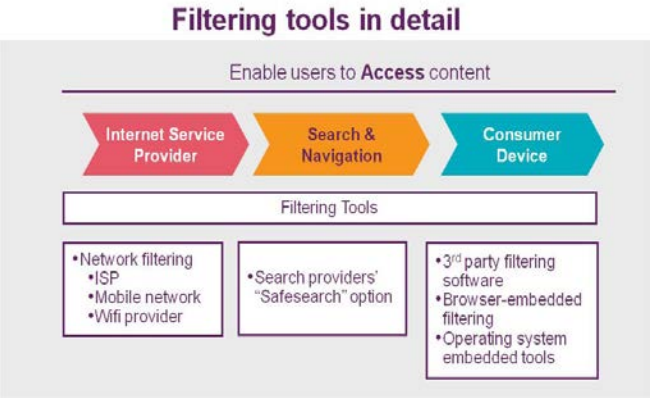
4.26 In some cases, children will be able to bypass filters, either by altering the filtering settings or by using tools to conceal the sites they are visiting from the filtering software. The main mechanisms by which filters may be bypassed are through the use of a VPN (virtual private network), which encrypts all internet traffic, and the use of proxy sites. In both cases, there are legitimate reasons for using such services – for example Google's language translation service can also be used as a proxy site and employees who work from home will typically be required to use a VPN to connect to their business IT systems. Although it may also be possible for a filtering tool to restrict the use of proxies and/or VPN services, this will not be appropriate in all homes or on all devices.

Filtering tools provided by ISPs, by search engines and on consumer devices

4.27 This section examines the specific characteristics of filters provided at different internet access points: by the ISP, by search engines and on consumer devices.

4.28 Filtering solutions can be installed either on a consumer device, such as a home PC, or at the network layer by the ISP; in addition, some search engines, including the market leader Google, offer a "safe search" option, which excludes sexually explicit images from appearing in search results.

4.29 Each type of filtering has advantages and disadvantages and is appropriate in different circumstances.



Network filtering

4.30 In the UK, some form of network-layer filtering is offered by some operators in all segments of the access market: fixed line internet access providers, mobile internet access providers and wifi providers:

- *Fixed line (home) internet access providers*: TalkTalk Group currently offers its subscribers a network filtering service, which aims to control the accessibility of potentially harmful sites and services on all devices in a home; BSkyB, BT and Virgin Media have all committed to offering a similar service by the end of 2013.

- *Mobile internet access providers*: Everything Everywhere, O2, 3 and Vodafone (and the mobile virtual network operators using their networks) all provide free adult content filtering for PAYG and contract mobile devices and dongles, either as default or by request.

- *Wifi providers*: O2, Virgin Media, Sky, Nomad, BT and Arqiva – which provide 90% of the UK's wifi hotspots – have also committed to providing filtered internet access "wherever children are likely to be present" in future; all of the listed providers already have filtering in place for some subscribers.

- *Domain Name Service* network filtering is also available. OpenDNS offers the Family Shield parental filtering service based on use of a modified domain name service, which excludes domains potentially harmful content (such as sexual material). However, changing DNS provider to implement Family Shield requires some technical competence and the use of alternative DNS providers is restricted by some major ISPs.

4.31 Network filtering offers the simplest way to secure comprehensive coverage of a child's internet experience. In particular, filtering for fixed line broadband promises coverage of all of the devices in a home with a single decision.

4.32 However, the fact that network filters apply to the whole home is a weakness as well as a benefit: in a house with adult, teenage and pre-teen internet users, filtering settings appropriate for the youngest users may limit other users' access excessively; and settings appropriate for older/adult users may not be sufficiently restrictive to protect the youngest. Similarly, adult users of wifi services may be frustrated by their inability to access lawful content which is blocked as being unsuitable for children.

4.33 As noted above, the second limitation of network filtering is that, typically, it does not deliver coverage of content accessed using apps. (Network filters can block content delivered outside the World Wide Web, for example via P2P file-sharing or on

newsgroups; but will do so en bloc, restricting access to legitimate and potentially harmful content accessed using these methods).

Search filtering

4.34 Some search engines, including Google, offer a “safe search” option, which excludes sexually explicit images from appearing in search results. Although safe search settings are often used by parents and it is possible to “lock” safe search settings on a browser using a password, they are relatively easy to bypass (for example by using an alternative search provider or alternative browser). This means they will primarily be relevant for parents of younger children.

Consumer device filtering

4.35 Parents can install control software on the individual devices their children may use to access the internet. Many PCs have pre-installed filtering tools and many ISPs (including BT, Sky and Virgin Media) offer free downloads of filtering software to their subscribers; parents also can download and install software themselves. Such controls may be part of a general security suite (e.g. Norton Antivirus) or focused on online child protection (e.g. Net Nanny).

4.36 These controls must be installed individually on each device. However, controls on PCs can be very flexible, offering a range of content categories to be restricted and allowing parents to create multiple accounts with different filtering settings.

4.37 Consumer device filtering is more complex for smartphones and tablets; there are not currently tools which allow the same simple level of control over the internet services accessible on a smartphone or tablet as exist for a PC. In order to filter services accessible on a smartphone or tablet, parents must put in place two types of control mechanism: one which restricts which apps can be installed on the device (ensuring that apps giving access to potentially harmful content cannot be installed) and used on the device; and secondly a restricted web browser which includes content controls (to limit access to potentially harmful content on the World Wide Web). There is a range of software packages which impose both of these restrictions, although the market is less well developed than for PC-based filtering.

4.38 Games consoles add further complexity to device level filtering. Most games platforms offer parents/carers the ability to restrict the playing of games discs based on age classification. Furthermore, there is an emerging market in dedicated games console apps e.g. Netflix on Xbox, web browsing capabilities, Skype, Facebook.

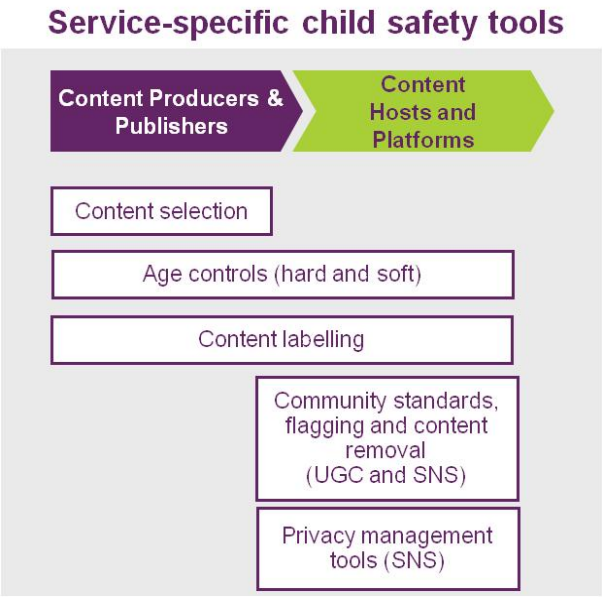
Filtering conclusions

4.39 In summary, content filtering is a valuable tool, used by a significant proportion of parents; but, in common with other tools and mechanisms used by parents, it cannot be relied upon, on its own, to protect children from harmful content online. Parents using filtering tools must be aware of the limitations as well as the advantages of such tools.

Service specific child safety tools

4.40 Filtering tools are intended to give comprehensive, or at least broad, coverage of internet sites and services; in addition to filtering, individual sites and services can help improve child internet safety through the provision of site-specific tools for their users – either the children themselves, or their parents. The tools individual providers

may offer are determined by the nature of their business. This section examines those tools laid out in the diagram below. (The term “SNS” indicates social networking sites and “UGC” indicates user generated content, which is generally content in the form of individual postings or self published channels on platforms such as YouTube).



Content producers and publishers

4.41 **Content producer/publishers** make decisions about what content to offer to their audiences; they may choose only to include content appropriate for children, ensuring that their entire service or site is child-safe. However, content providers will more typically wish to offer content appropriate for a wider range of audiences or for adults only. These publishers can help improve safety by offering *content labels* and/or *age control mechanisms*.

Content labelling

4.42 Content providers can classify and label their own content, potentially using a range of different measures, from age-rating through to specific warnings about drugs, violence and sexually explicit content. Services are also availing themselves of industry standard classification services such as the British Board of Film Classification ratings system to inform users of content suitability. Similarly, the Pan European Games Information (PEGI) scheme also provides age-ratings for games and apps. Users can refer to these labels directly to avoid content which is likely to be unsuitable; or the labels can be used in combination with an age control mechanism.

Age control mechanisms

4.43 An *age control mechanism* is intended to secure that users outside a specified age range will not have access to a site or service as a whole; or to some of the content within a site or service.

Age controls: self declaration and guidance

4.44 Many Video-on-Demand services operated by UK broadcasters offering "TV catch up services" offer voluntary "soft" age verification – relying on a user's self-declared report of their age to access material which the service provider has given guidance on as unsuitable for those under 16. For example, the BBC iPlayer allows parents to restrict the accessibility of content, with the restrictions applying to programmes which are unsuitable for those under 16.

4.45 Some providers who offer "soft", self-declared age control mechanisms will also allow parents to lock the controls in place. A parent can turn on the age control mechanism on the iPlayer and lock it on with a password; everyone who uses that browser, on that device, will be subject to the age restrictions. Such measures may be relatively easy to bypass by an informed child, either by using a different web browser or by clearing cookies[23].

Age controls: compulsory content access controls

4.46 In the UK, regulated Video-on-Demand services (which are regulated by ATVOD, see Annex 1 for more detail) must ensure that material which is likely to seriously impair the physical or moral development of minors, typically R18 equivalent sexually explicit content, may only be seen by those users able to demonstrate that they are older than 18. This may be secured by, for example, requiring passport or driver's licence details to be provided or requiring proof of ownership of an age-restricted payment mechanism like a credit card, before access to such content is permitted.

Content hosts and platforms

4.47 **Content hosts and platforms** are a particularly important group of online service providers including some of the most popular sites among children, such as social networking sites such as Facebook, and content hosting sites like YouTube. Social networking sites are also important because they are a platform for interaction and communication. As well as offering content labelling and age controls, content hosts and platforms can operate community standards and content removal processes; finally, social networking sites, which allow users to communicate and to share personal data, may help children and their parents manage risks through privacy management tools.

Content labelling

4.48 Content hosts do not select the content whose publication they enable: the content is chosen and posted or uploaded by their users. However, some content hosts do allow their users to rate or label content, for example as being inappropriate for children. As is the case for content publishers' labels, these may serve either as warnings to potential viewers, or as an input to age control mechanisms also offered on the site. For example, YouTube allows professional content providers (in the TV and Movies sections of the site) to apply language, nudity, sexual situations, violence and drug use labels; and everyone who publishes content on the site must specify whether it is suitable for adult viewers only (18+).

[23] A ***cookie*** is a small text file sent by a website to a user's web browser, and stored on the user's local hard drive. Cookies serve many purposes, of which the simplest is to allow a page to be customised, but they can also be used to track the behaviour of a user.

Age control mechanisms

4.49 Some hosting service providers offer age control mechanisms; these are mostly *soft* controls – only requiring that users self-declare their age and hence the categories of content or the services which may be appropriate (e.g. most social networking sites specify a minimum age). In addition, some hosting services, such as YouTube, allow parents to lock an age-control in place on a browser using a password.

Community standards and content removal

4.50 Although they do not review all of the content which their users publish, many content hosting and social networking sites have *community standards* which define when content is unacceptable on the site. These typically include prohibitions on personal attacks, harassment, abuse or discrimination of any kind; rules around the posting (and sometimes prohibition) of sexual content; restrictions around the posting of violent content; the prohibition of posting material that encourages self-harm; respect for individuals' privacy; and the prohibition of material that could incite crime, violence or could be considered illegal.

4.51 In order to maintain and enforce such standards, three distinct – and sometimes complementary – types of moderation approach are commonly used. *Pre-moderation* sees all content submitted by users checked by a moderator before it goes live and appears on a particular site. A *post-moderation* approach involves all content submitted by users being checked by a moderator as soon as the content goes live (or shortly afterwards). *Reactive* moderation leaves content submitted by users unchecked before it goes live, relying on user generated reports to a moderator of potential activities breaking a site's community standards and/or terms and conditions.

4.52 In the majority of cases, these standards are enforced on a reactive basis, where users report ("flag") content they believe breaches the standards for the site and the site operator will review the reports and remove content which they consider to break the relevant rules. The tools for reporting content can vary from reporting buttons that relate to a particular piece of content (for example, a post, photo or video) to buttons which "flag" the conduct of an individual user or account, depending on the nature of the site. In the event that a user is found repeatedly to break the rules, their account may be deleted.

4.53 Some sites - such as the Huffington Post (which uses pre- and reactive moderation) and the BBC Message Boards (which uses all three approaches) – may use a combination of moderation approaches.

4.54 There is an additional emerging type of content provision accessed through "apps" on mobile devices such as smartphone and tablets. An app is the generic term for a software programme, typically for a device like a smartphone or tablet, enabling a specific function, such as playing a game, online banking or social networking. App stores, frequently branded and linked to particular devices, are most commonly used to find and download apps. Some stores, such as Apple's, aim to review and maintain technical and editorial standards for the apps they distribute – akin to a content publisher – but do not create or commission (most) apps themselves, or accept responsibility for the quality of the apps they distribute. In this respect could be seen to act in the same way as a content host.

4.55 Apple operates a prior review process for its app store: apps are rated for age-groups, and those found to include sexually explicit material are rejected; Google

allows app developers to rate content themselves and will remove sexually explicit content when informed about it. However, it is possible on some devices to use alternative stores – and hence to bypass the controls which the store operators seek to impose.

4.56 In addition to action within the boundaries of their own site, some service providers enable users to report abuse directly to the relevant authorities. For example, there is a "ClickCEOP" button on some sites which children use; this is a sort of "panic button" which allows users to report inappropriate behaviour such as sexual chat or being asked to do things which make the user feel uncomfortable. The button links to the CEOP centre run by the police.

4.57 The community standards and the speed and effectiveness of (i) the community in flagging inappropriate content and (ii) the site operator in acting on such complaints, may be an important consideration for parents in deciding whether to allow their children access to specific hosting and social networking sites.

Privacy management tools

4.58 Social networking sites are also a source of contact and conduct risks to children, because they enable children to publish content, potentially including personal information, and to communicate with others. Typically, a social networking site will offer a range of options, critical among which will be:

- Publication and profile settings. Adjusting these on individual accounts allows users to determine who among the users of the site and the wider internet audience can see the information a user is sharing, and with whom they can communicate. Some social networking sites have specific settings intended to enhance the safety of children: for example, by default the information shared by a Facebook user between the ages of 13 and 17 is only visible to that user's group of friends. Adult users' posts are accessible to everyone.

- Communication settings – for example, who can make a friend request to a user: for example, Facebook allows this to be limited to "friends of friends".

4.59 However, the impact of these tools on children's safety depends on appropriate use of the settings. As set out in the research section, children do not always actively choose an appropriate level of privacy within their profile settings and parents should be prepared to advise on and consider monitoring the social networking site settings of their children, in order to ensure that contact risks are appropriately minimised.

Section 5

Part 2 The Research

Children and the internet: use and concerns

5.1 This part of the report provides qualitative and quantitative insight around three specific areas:

i) Take-up, awareness of and confidence of parents in relation to parental controls and the broader strategies parents may adopt to improve children's online safety;

ii) Levels of parental awareness and confidence with the safety measures which may be in place on sites regularly visited by children including, but not restricted to, content providers, search engines and social networking sites;

iii) Why parents may choose not to apply parental control tools.

Methodology

5.2 The findings reported in this part of document are drawn from:

- **The 2013 Children and Parents: Media Use and Attitudes report**[24]
  This report provides a detailed examination of media literacy among children and young people[25] aged 5-15 and their parents/carers[26], as well as an overview of media use by children aged 3-4[27]. The 2013 survey was carried out among over 1600 children and 2300 parents. The survey was first carried out in 2005 and so it is possible to track trends over time in many areas.

- **The 2012 Parents' views of parental controls report**[28]
  This qualitative report provides a more nuanced understanding of the rationale for parents' usage or non usage of, and attitudes to, parental controls to complement the existing quantitative data.

  The focus of this study was on parents of children aged between 5 and 15, with a weighting towards 8-11 and 12-15 year olds. An equal number of those with and without parental controls were represented, and a small number of lapsed users were included. A number of research methods were used, including extended in-home family interviews, some of which included children, as well as 'standard' mini-groups and 'friendship' mini-groups. The sample spanned all UK countries and had both urban and rural coverage. In total, close to 100 people[29] took part during July 2012.

[24] http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/october-2013/research07Oct2013.pdf.
[25] References to children in this report are used to refer to children and young people.
[26] References to parents in this report are used to refer to parents and carers.
[27] www.ofcom.org.uk/medialiteracyresearch.
[28] http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2012/Annex_1.pdf.
[29] A total of 85 parents and 10 children took part in this research.

Key Findings

- Children's preference for internet-enabled devices reflects changes in how they are going online and what they are doing online. The multi-functionality of tablets appears to meet younger children's entertainment needs – for watching audio-visual content and playing games – older children's use of smartphones focuses around peer communication.
- There has been a decrease since 2012 in the proportion of children across the age ranges with an active profile on main social media sites.
- Children's confidence in using internet resources is high but there have been some decreases in children's online safety skills in relation to the visibility of social networking profiles, and knowledge of how to block unwanted online messages.
- Content related risks are of less concern to parents than contact or conduct related risks.
- Most parents of 5-15s who go online at home trust their child to use the internet safely (83%), and feel that the benefits of the internet outweigh the risks (70%).

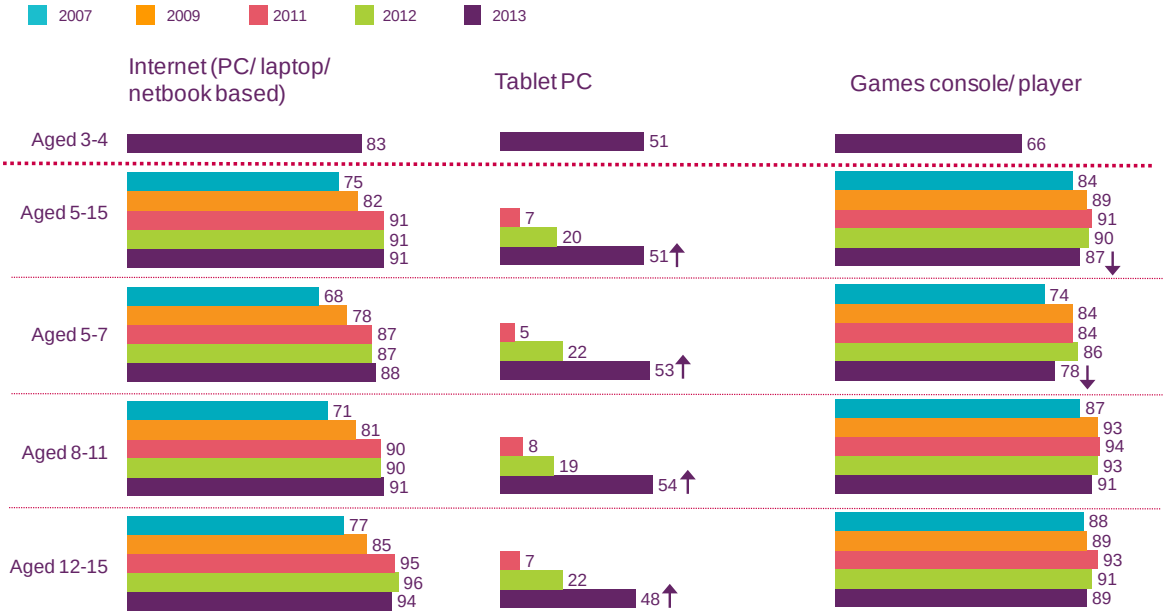
Children's access and use of the internet

5.3 To better understand parental online mediation strategies and levels of parental awareness and confidence in safety measures in place on the sites regularly visited by children, it is useful to consider some of the key changes in children's use of the internet, and the current attitudes and concerns of both children and parents.

5.4 Tablets are becoming the must-have device for children while older children opt for smartphones.

5.5 Figure 1 shows that household ownership of a tablet has more than doubled since 2012 (51% vs. 20%) but use of a tablet computer at home has tripled among 5-15s since 2012 (42% vs.14%) and one-quarter (28%) of 3-4s use a tablet computer at home.

Figure 1: Availability of key platforms in the home, by age: 2007, 2009, 2011, 2012 and 2013

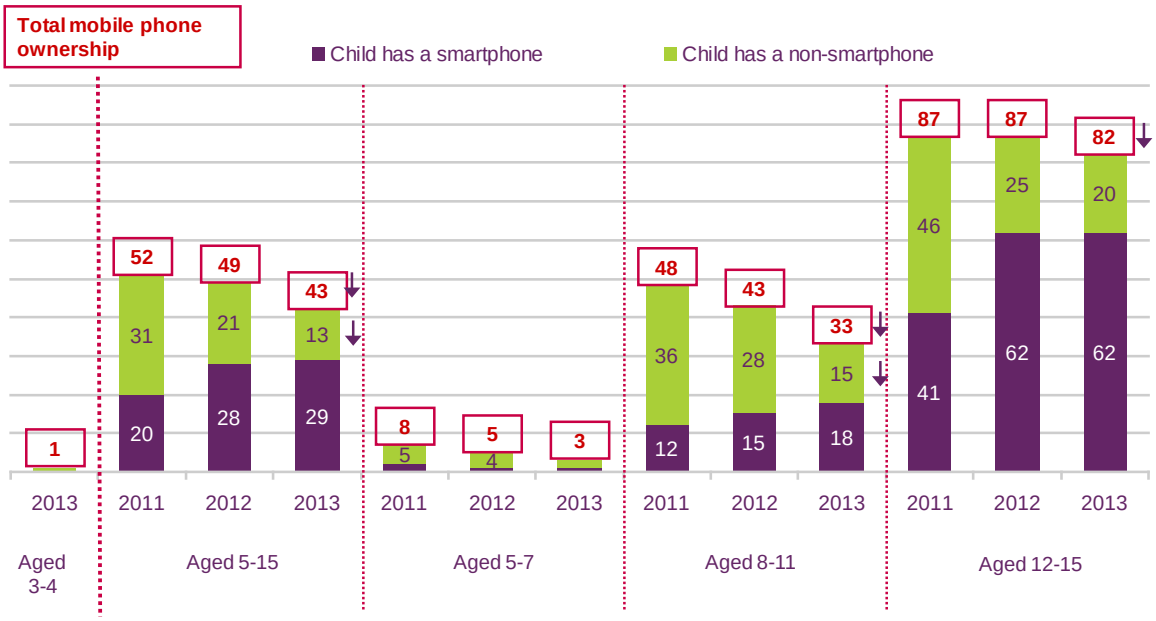


QP3/C/E/H/I – I'm going to read out a list of different types of equipment that you may or may not have in your home, and which your child may or may not use (prompted responses, single coded)
Base: Parents of children aged 3-4 or 5-15 (685 aged 3-4 in 2013, 3696 aged 5-15 in 2007, 2131 aged 5-15 in 2009, 1717 aged 5-15 in 2011, 1717 aged 5-15 in 2012, 1689 aged 5-15 in 2013, 985 aged 5-7 in 2007, 576 aged 5-7 in 2009, 573 aged 5-7 in 2011, 570 aged 5-7 in 2012, 533 aged 5-7 in 2013, 1354 aged 8-11 in 2007, 774 aged 8-11 in 2009, 586 aged 8-11 in 2011, 575 aged 8-11 in 2012, 587 aged 8-11 in 2013, 1357 aged 12-15 in 2007, 781 aged 12-15 in 2009, 558 aged 12-15 in 2011, 572 aged 12-15 in 2012, 569 aged 12-15 in 2013) - significance testing shows any differences between 2012 and 2013.
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

5.6 This preference for internet-enabled devices is reflected in children's choice of mobile phones. Figure 2 below shows that among children aged 5-15 mobile ownership has decreased to 43%. This is a decline of 6 percentage points since 2012, driven by a 10 percentage point decline in ownership for 8-11s (33% vs. 43%) and a 5 percentage point decline for 12-15s (82% vs. 87%). However, smartphone ownership has remained stable for 8-11s (18%) and 12-15s (62%).

5.7 In contrast, children aged 5-15 are now less likely to have a games console/player in their bedroom (47% vs. 56%). This reflects a decline in the use of fixed and handheld games players (81% vs. 86%) compared to a threefold increase among 5-15s in using tablet computers to play games (23% vs. 7%).

Figure 2: Smartphone and non-smartphone ownership, by age: 2011, 2012 and 2013



QP3F/ QP4 - I'm going to read out a list of different types of equipment that you may or may not have in your home, and which your child may or may not use (prompted responses, single coded)/ You mentioned that your child has their own mobile phone. Is this a Smartphone? A Smartphone is a phone on which you can easily access emails, download files as well as view websites and generally surf the internet. Popular brands of Smartphone include iPhone, BlackBerry, Nokia Lumia and Android phones such as HTC or Samsung Galaxy. (spontaneous responses, single coded)
Base: Parents of children aged 3-4 or 5-15 (685 aged 3-4 in 2013, 1717 aged 5-15 in 2011, 717 aged 5-15 in 2012, 1689 aged 5-15 in 2013, 573 aged 5-7 in 2011, 570 aged 5-7 in 2012, 533 aged 5-7 in 2013, 586 aged 8-11 in 2011, 575 aged 8-11 in 2012, 587 aged 8-11 in 2013, ,558 aged 12-15 in 2011, 572 aged 12-15 in 2012, 569 aged 12-15 in 2013) - significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Devices used 'mostly' by children to go online at home

5.8 Figure 3 shows that children mostly accessing the internet via a laptop/netbook/PC has decreased to 68% – down from 85% in 2012. In contrast, the number of children who are now mainly using an alternative device to go online has doubled to 32%, from 15% in 2012, with tablets (13%) and mobiles (11%) the most popular devices.

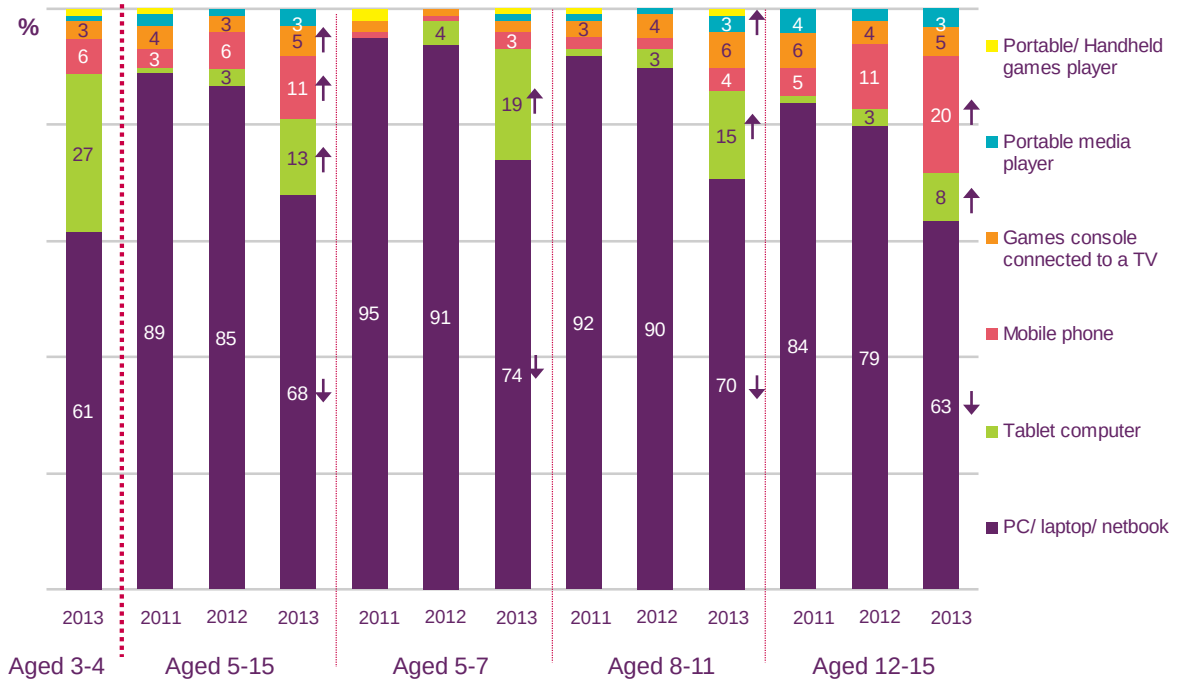
5.9 Almost a quarter of children are using tablets to go online – nearly three times as many as last year (23% vs. 9%). Over half of 12-15s use a mobile phone to go online at home (52% vs. 44% in 2012).

5.10 Younger children who go online at home, in particular, are five times more likely than in 2012 to mostly use a tablet computer (19% vs. 4% for 5-7s, 15% vs. 3% for 8-11s). One in eight 3-4s use a tablet computer to go online (12%).

5.11 Half of children aged 12-15 say they use the internet on their own most of the time. One in ten internet users aged 5-7 (11%) and one-quarter aged 8-11 (24%) use the internet on their own most of the time.

5.12 The majority of 5-7s and 8-11s say they spend most of the time using the internet with an adult in the room (85% and 69% respectively).

Figure 3: Devices used 'mostly' by children to go online at home, by age: 2011, 2012 and 2013



QP26B – And when your child goes online at home, which device do they mostly use? (prompted responses, single coded)
Base: Parents of children aged 3-4 or 5-15 whose child ever goes online at home (219 aged 3-4 in 2013,1421 aged 5-15 in 2011, 1424 aged 5-15 in 2012, 1429 aged 5-15 in 2013, 396 aged 5-7 in 2011, 376 aged 5-7 in 2012, 381 aged 5-7 in 2013, 496 aged 8-11 in 2011, 495 aged 8-11 in 2012, 497 aged 8-11 in 2013, 529 aged 12-15 in 2011, 553 aged 12-15 in 2012, 551 aged 12-15 in 2013). ***In 2013 responses are taken from the child aged 12-15 rather than the parent, as had been the case in previous years - Significance testing shows any change between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Children's internet activities

5.13 Schoolwork/homework is the most commonly-mentioned internet activity carried out at least weekly (75%) by 8-11s, followed by games (54%) and information (45%).

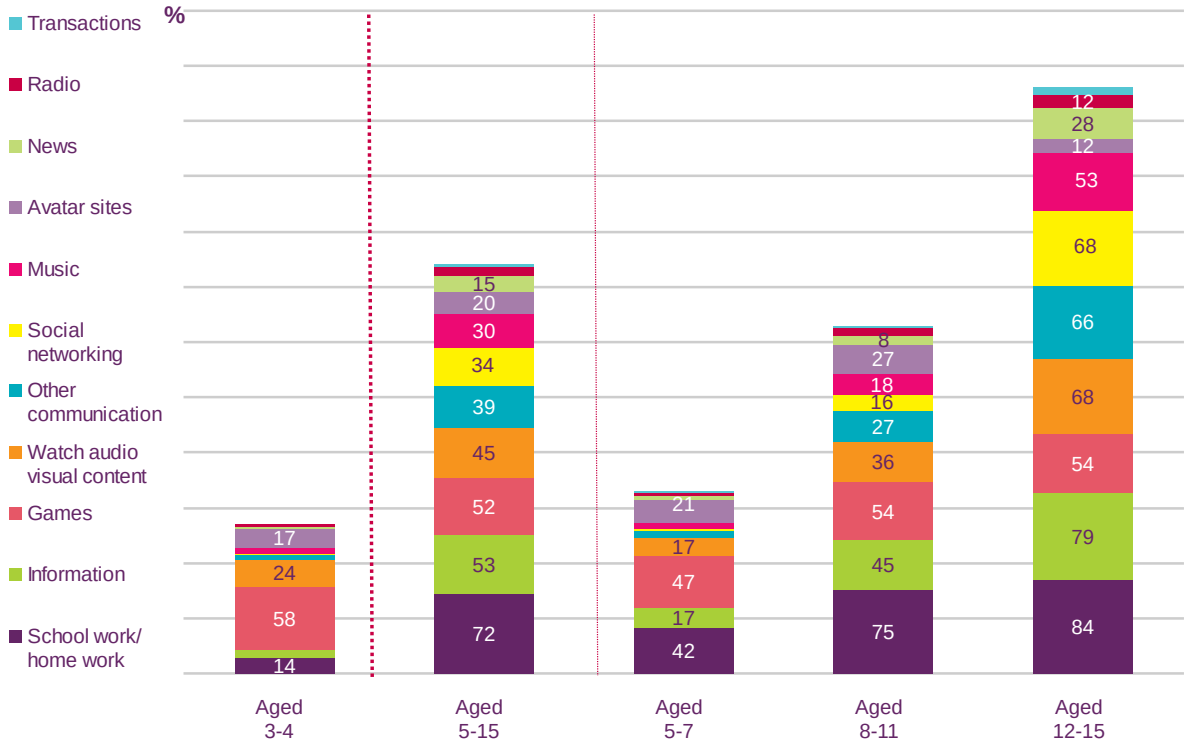
5.14 However, children aged 8-11 are now more likely to use the internet weekly for making/receiving telephone or video calls using services like Skype or FaceTime[30] (10% vs. 5%) and for going to photo-sharing websites such as Flickr, Instagram and Snapfish (5% vs. 2%). They are less likely to use the internet at least weekly for avatar websites (27% vs. 36%) as are 5-7s (21% vs. 33%).

5.15 Games are the most commonly-mentioned online activity carried out at least weekly by the majority of 3-4s (58%).

5.16 As shown in Figure 4, schoolwork/homework is the most commonly-mentioned internet activity among 12-15s (84%), followed by information (79%), social networking (68%) and watching audio-visual content (68%). A majority of 12-15s also go online weekly for other communication (66%), for games (54%) and for music (53%).

[30] Prior to 2013, making or receiving telephone or video calls using services like Skype or FaceTime only referred to telephone calls (and not video calls) on Skype and did not reference FaceTime. This may affect the responses given and any trend data for this particular online activity.

Figure 4: Types of use of the internet by users at least weekly, by age: 2013



QC14A-U – When you're at home, do you use the internet on any type of computer, mobile phone or games player to do any of these things? (prompted responses, single coded) – PERCENTAGES SHOWN REFLECT THOSE THAT UNDERTAKE ACTIVITY AT LEAST WEEKLY
Base: Children aged 5-15 who use the internet at home (219 aged 3-4, 1426 aged 5-15, 381 aged 5-7, 497 aged 8-11, 548 aged 12-15).
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

5.17 In 2013, children aged 12-15 with a smartphone are more likely than in 2012 to use their phone at least weekly for four activities: looking at videos or clips posted by other people on sites like YouTube (50% vs. 36%), sending/receiving photos (38% vs. 30%), putting photos or videos on sites like YouTube, Facebook or Instagram for others to see (33% vs. 17%) and watching TV programmes or clips (23% vs. 16%).

5.18 Smartphone users send an estimated 184 instant messages in a typical week and smartphones are the most popular device for accessing social networking sites among 12-15 year olds with four in ten (41%) 12-15s saying they mostly use a mobile phone to visit their main social networking site profile.

5.19 Children aged 12-15 are still twice as likely to say that, of all the media they use regularly, they would most miss their mobile phone (39%), compared to the next most-missed media: using the internet (19%) and watching television (19%). This rises to half (51%) of 12-15s with a smartphone.

5.20 Thirty seven per cent of 5-15s who play games have ever played games online. There has been an increase in the numbers of younger children playing games online in the last year with 24% of 5-7s (up from 18% in 2012) and 36% of 8-11s (up from 29% in 2012) now playing games online.

5.21 One in ten children aged 3-4 who play games at all play games online at home (12%).

5.22 The majority of children in each age group who play games online play on their own/against the computer or games player, accounting for over four in five 5-7s (86%), close to seven in ten 8-11s (68%) and seven in ten 12-15s (73%).

Children's use, attitudes and concerns around sites regularly visited

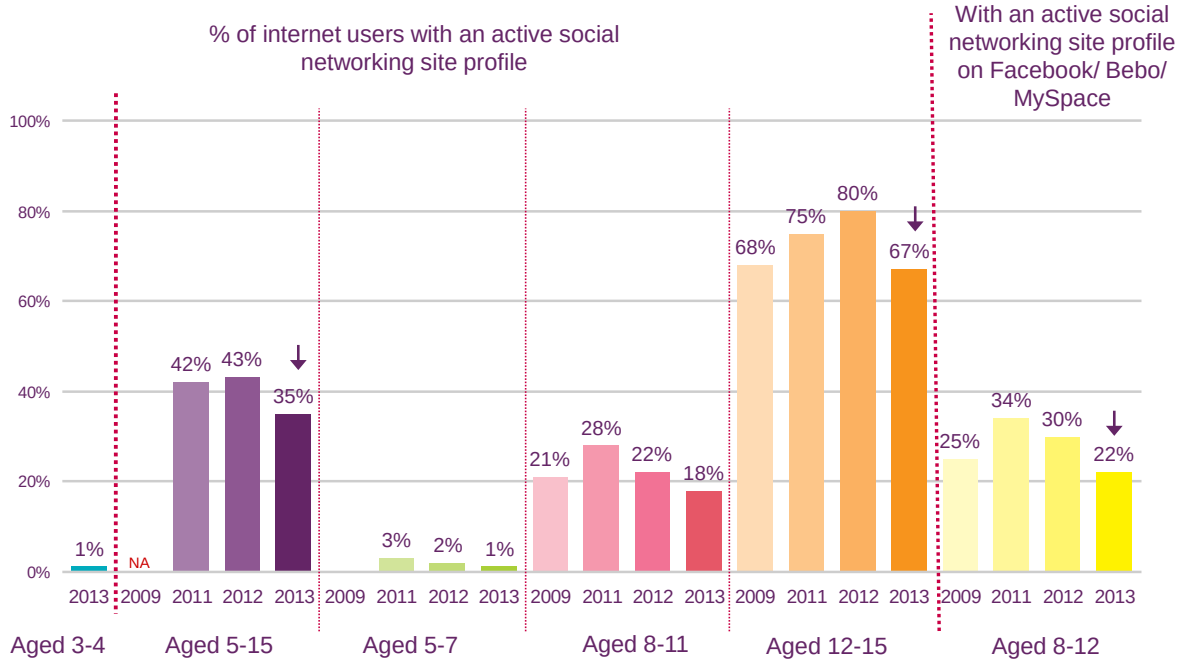
5.23 Compared to last year, 12-15s are now less likely to say they have set up a social networking site profile (68% vs. 81%). There has also been a decrease since 2012 in the proportion of children aged between 8-12 (under-age users) with an active profile on Facebook/Bebo or MySpace (22%; down from 30% in 2012), as illustrated in Figure 5.

5.24 Figure 6 shows that nearly all 12-15s with an active social networking profile continue to use Facebook (97%). Since 2012 they are less likely to have a profile on Bebo (4% vs. 8%) and more likely to have a profile on Twitter (37% vs. 25%).

5.25 Boys are more likely than girls to have an active profile on YouTube (31% vs. 21%), while girls are three times more likely to have a profile on Tumblr (12% vs. 4%). As a proportion of all children (as distinct from those who use the internet at home), 24% of all 12-15s have a profile on Twitter, compared to 62% of all 12-15s with a Facebook profile.

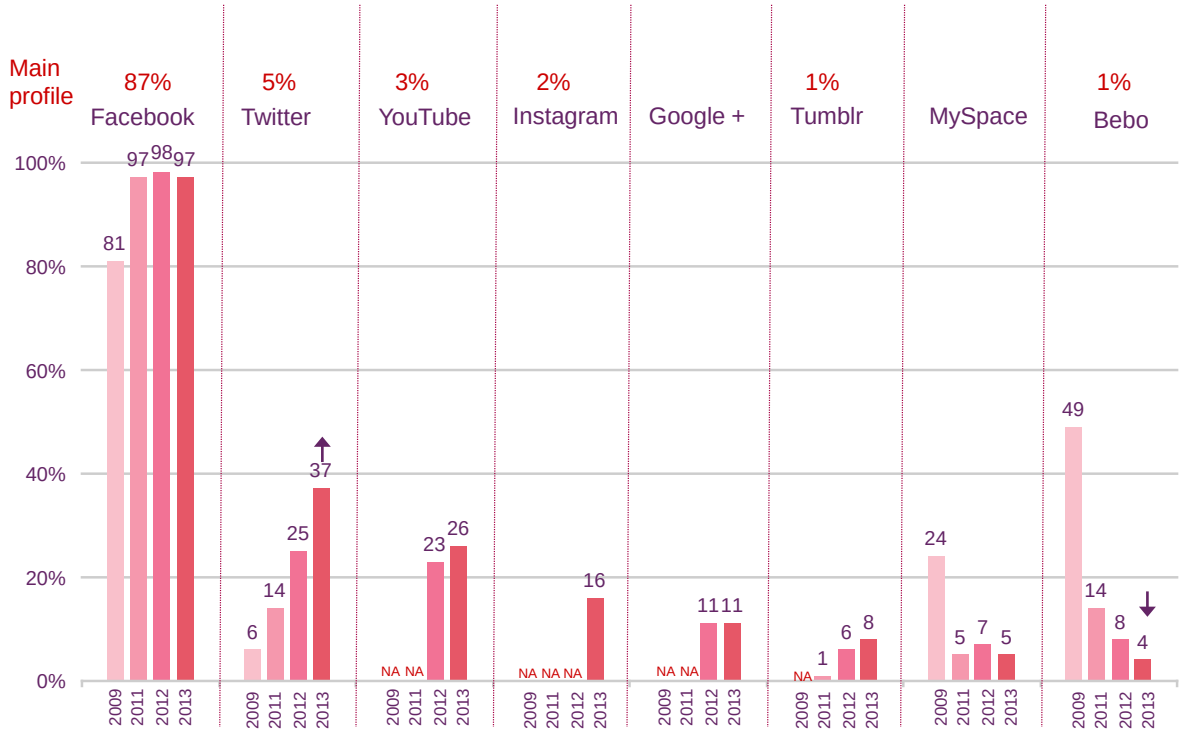
5.26 Of those 12-15s with an active social networking profile, the vast majority (85%) access their main social networking site profile every day and 20% do so more than ten times a day. This figure increases to 27% among those 8-15s who access their profile mainly on any type of mobile phone.

Figure 5: Incidence of children with an active social networking site profile, by age: 2009, 2011–2013



QP45A/ QC21A– Which different social networking sites do you have a page or profile on? (spontaneous responses, multi coded)
Base: Parents of children aged 3-7 and children aged 8-15 who use the internet at home (219 aged 3-4 in 2013, 1421 aged 5-15 in 2011, 1424 aged 5-15 in 2012, 1426 aged 5-15 in 2013,396 aged 5-7 in 2011, 376 aged 5-7 in 2012, 381 aged 5-7 in 2013, 581 aged 8-11 in 2009, 496 aged 8-11 in 2011, 495 aged 8-11 in 2012, 497 aged 8-11 in 2013, 645 aged 12-15 in 2009, 529 aged 12-15 in 2011, 553 aged 12-15 in 2012, 548 aged 12-15 in 2013, 746 aged 8-12 in 2009, 655 aged 8-12 in 2011, 678 aged 8-12 in 2012, 677 aged 8-12 in 2013) Significance testing shows any changes between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Figure 6: Social networking websites where children aged 12-15 currently have an active profile: 2009, 2011, 2012 and 2013 (of those with an active profile)



QC21A– Which different social networking sites do you have a page or profile on? (spontaneous responses, multi coded) – showing responses of 2% or more of children aged 12-15 with a current social networking site profile
Base: Children aged 12-15 who have a current social networking site profile (442 aged 12-15 in 2009, 407 aged 12-15 in 2011, 446 aged 12-15 in 2012, 378 in 2013). Significance testing shows any changes between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Children's online confidence and understanding

5.27 The vast majority of 8-15s say that they are confident about their online activities. Eighty-three per cent of 8-11s and 91% of 12-15s say that they are confident about how to stay safe online and 67% of 12-15s say they are confident that they can judge whether websites are truthful.

5.28 To put this in context, a majority of 8-11s (61%) say they only visit websites they've visited before, compared to slightly less than half of 12-15s (49%). Among 12-15s, boys are more likely than girls to say they visit lots of websites they haven't visited before (13% vs. 5%).

5.29 Forty-five per cent of 12-15s who ever use search engines make a critical judgement about search engine results, thinking that some of the sites returned will be truthful and some won't be. Thirty-two per cent believe that information on a website listed by a search engine must be truthful.

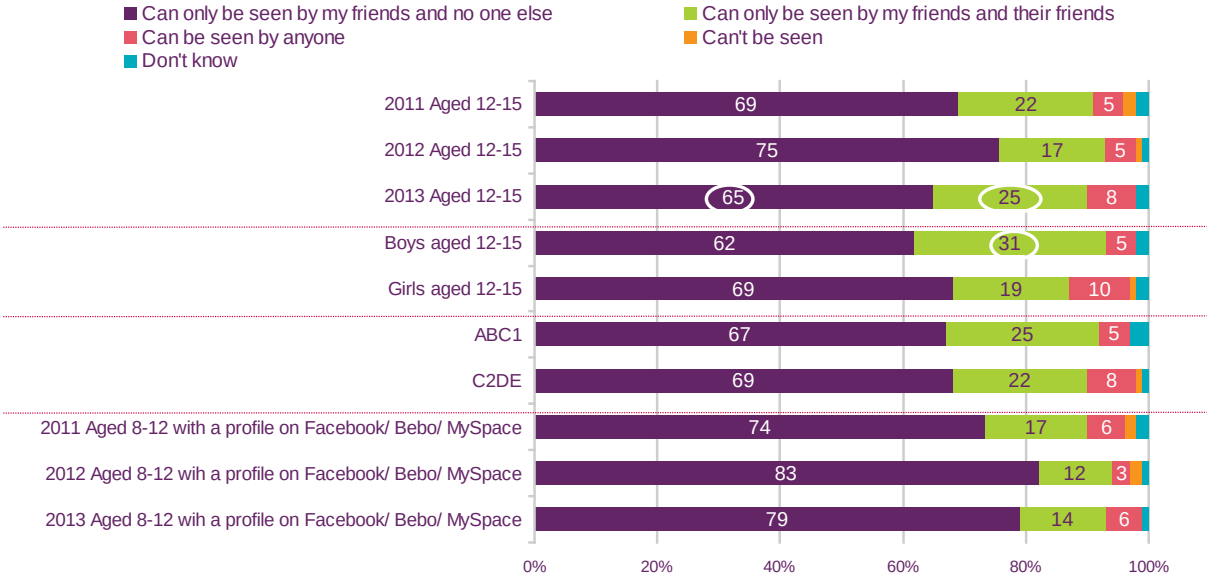
5.30 Close to half (48%) of 12-15s, after being provided with a description of online personalised advertising, said they were aware of this practice, although a majority (53%) are either unsure how they feel about it or feel it's neither a good nor a bad thing.

5.31 However, there have been some decreases in children's online safety skills. On average, 12-15s have never met, in person, three in ten (on average, 78) of the

friends listed on their main social networking site profile. Most children aged 12-15[31] with an active social networking profile say that their profile can be seen only by their friends (65%), while around one in 12 say it can be seen by anyone (8% for 12-15s).

5.32 As illustrated in Figure 7, a substantial minority of 12-15s have a social networking profile which may be visible to people not known to them, and this has increased since 2012 (33% vs. 22%).

Figure 7: Visibility of social networking site profiles, by age: 2011–2013



QC24 – And do you know if this profile can be seen by other people?(Prompted responses, single coded)
Base: Children aged 8-15 who have a social networking site profile that is currently active (403 aged 12-15 in 2011, 446 aged 12-15 in 2012, 378 aged 12-15 in 2013, 178 boys aged 12-15, 200 girls aged 12-15, 214 ABC1, 249 C2DE, 221 aged 8-12 with a profile on Facebook/ Bebo /MySpace in 2011 228 aged 8-12 with a profile on Facebook/ Bebo /MySpace in 2012, 168 aged 8-12 with a profile on Facebook/ Bebo /MySpace in 2013). Significance testing shows any changes between 2012 and 2013 and between boys and girls aged 12-15 and between ABC1 and C2DE in 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

5.33 Children with a social networking site profile that may be visible to people not known to them are more likely to have undertaken some kind of potentially risky online behaviour, such as adding people to their contacts they don't know in person, or sending photos or personal details to people only known online.

5.34 However, more positively, compared to 2012, only a very small number of 8-15s now say they would not tell someone if they found something online that was worrying, nasty or offensive (1% vs. 3% for 8-11s, and 4% vs. 8% for 12-15s).

5.35 Figure 8 shows that compared to 2012, children aged 12-15 are less likely to know how to block messages from someone they don't want to hear from (53% vs. 68%) and to have done this in the past year (32% vs. 42%).

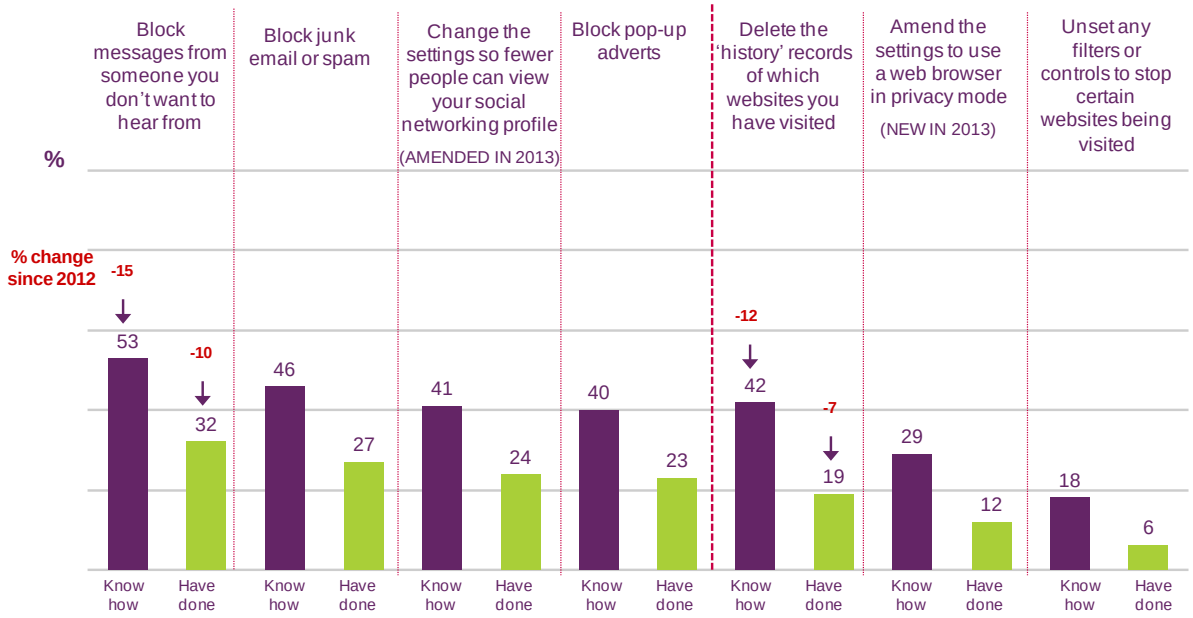
5.36 Less than half of 12-15s know how to block junk email or spam (46%), change settings on their social networking site profile so fewer people can view the profile (41%), or block pop-up adverts (40%). About one in four claim to have amended their social networking site profile settings (24%) or blocked pop-up adverts (23%).

5.37 Forty-two per cent of 12-15s know how to delete their browsing history and 19% claim to have done this in the past year. Around one in five (18%) know how to disable online filters or controls, but considerably fewer (6%) have done this in the

[31] Low base sizes prevent analysis among 8-11s.

past year. Three in ten (29%) know how to amend settings to use a web browser in privacy mode and one in eight claim to have done this (12%).

Figure 8: Experience of 'safe' and 'risky' online measures among children aged 12-15: 2013



QC59A/B– Please take a look at the list of things shown on this card and think about whether you know how to do any of these things online. Please read out the letters on the card if you know how to do this./ And are there any things on this list that you personally have done online in the last year? Please read out the letters on the card if you have done this in the last year. (Prompted responses, multi coded)
Base: Children aged 12-15 who use the internet at home or elsewhere (565 aged 12-15) – Significance testing shows any difference between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

5.38 Figure 9 shows that 15% of 12-15s have participated in any of a list of four potentially risky things we asked about. One in ten children aged 12-15 (9%) say they have taken the contact details of someone they have met only online, and around one in 20 (5%) have sent personal information to a person they have only had contact with online.

5.39 Among children aged 12-15 with an active social networking profile, children with more open profiles (whose profile is set to be seen by anyone or by friends of friends) are more likely than children with more private profiles (which can be seen only by their friends) to have: added people who they have only had contact with online to their friends list (28% vs. 6%); sent personal information to a person they have only had contact with online (10% vs. 4%); or sent a photo or video of themselves to a person they've only had contact with online (9% vs. 2%).

Figure 9: Experience of potentially risky online behaviour among children aged 12-15: 2011–2013

QC58 – Please take a look at the list of things shown on this card and think about whether you have done any of these things in the last year. If there is something on the list that you have done in the last year then please just read out the letters from the card. please just read out the letters from the card if you yourself have experienced any of these things in the last year. (Prompted responses, multi coded)
Base: Children aged 12-15 who use the internet at home or elsewhere (550 aged 12-15 in 2011, 568 aged 12-15 in 2012, 565 aged 12-15 in 2013) - significance testing shows any difference between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

5.40 As illustrated in Figure 10, around nine in ten children aged 8-11 (88%) or 12-15 (94%) recall receiving any information or advice about staying safe online.

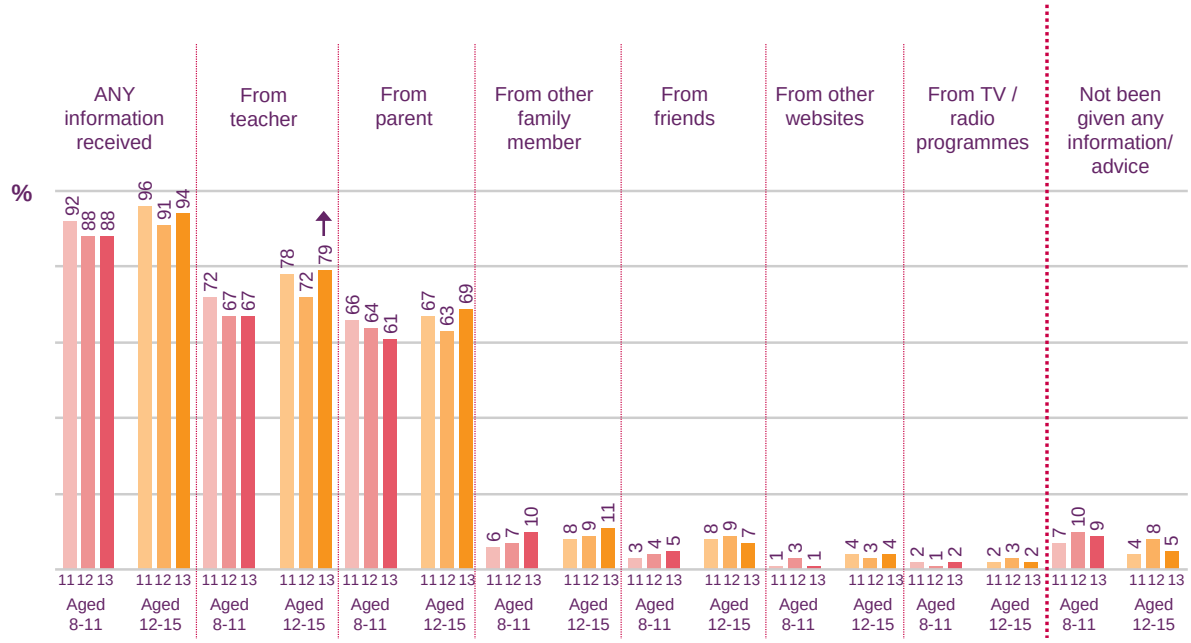
5.41 For both age groups this information is most likely to be recalled as being from a teacher (67% for 8-11s and 79% for 12-15s). More than six in ten in each age group recall receiving this information from a parent[32] (61% for 8-11s, 69% for 12-15s) and around one in ten from other family members (10% for 8-11s and 11% for 12-15s). Other sources of this information are nominated by less than one in ten children in either age group, with 12-15s more likely than 8-11s to recall receiving information or advice from other websites (4% vs. 1%).

5.42 Seven per cent of 8-15s say they have not been given any information or advice, and this is more likely for 8-11s than 12-15s (9% vs. 5%).

5.43 While girls aged 12-15 are no more likely than boys to recall receiving any information or advice overall (95% for girls vs. 92% for boys), they are more likely to recall receiving advice from a parent (75% vs. 63%). There are no differences by gender for 8-11s.

[32] These incidences are lower than those reported at Figure 31 and Figure 32. This could be attributable to the different way in which the question was asked of parents (through a prompted list of responses) and of children (through unprompted/spontaneous responses). One in four children aged 8-15 who go online at home, whose parents say they have ever talked to them about staying safe online, do not name their parent as a source of advice (27%).

Figure 10: Children stating they have been given any information or advice about staying safe online, by age: 2011–2013



QC35 – Have you ever been given any information or advice about how to stay safe when you are online? (spontaneous responses, multi-coded)
Base: Children aged 8-15 who use the internet at home or elsewhere (563 aged 8-11 in 2011, 539 aged 8-11 in 2012, 554 aged 8-11 in 2013, 550 aged 12-15 1in 2011, 568 aged 12-15 in 2012, 565aged 12-15 in 2013). Significance testing shows any difference between 2012 and 2013.
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Children's online concerns and dislikes

5.44 The incidence of children disliking seeing things online that are too old for them, or things that make them feel sad, frightened or embarrassed, has decreased since 2012 for both 8-11s (15% vs. 23%) and 12-15s (10% vs.15%).

5.45 One in five 12-15s dislike people being nasty, mean or unkind to each other (21%). The 12-15s are also more likely than 8-11s to be concerned about bad things that people have written about them, or photos of them on their profile page (11% vs. 6%).

5.46 Fifteen per cent of 8-11s and 10% of 12-15s dislike seeing things online that are too old for them or things that make them feel sad, frightened or embarrassed.

5.47 Almost one in ten 12-15s (8%) and 4% of 8-11s say they have experienced online bullying in the past year. Close to half of all 12-15s know someone with experience of negative online/mobile phone activity such as online bullying, gossip being spread or embarrassing photos being shared. One in five say they have personal experience of negative online/mobile phone activity.

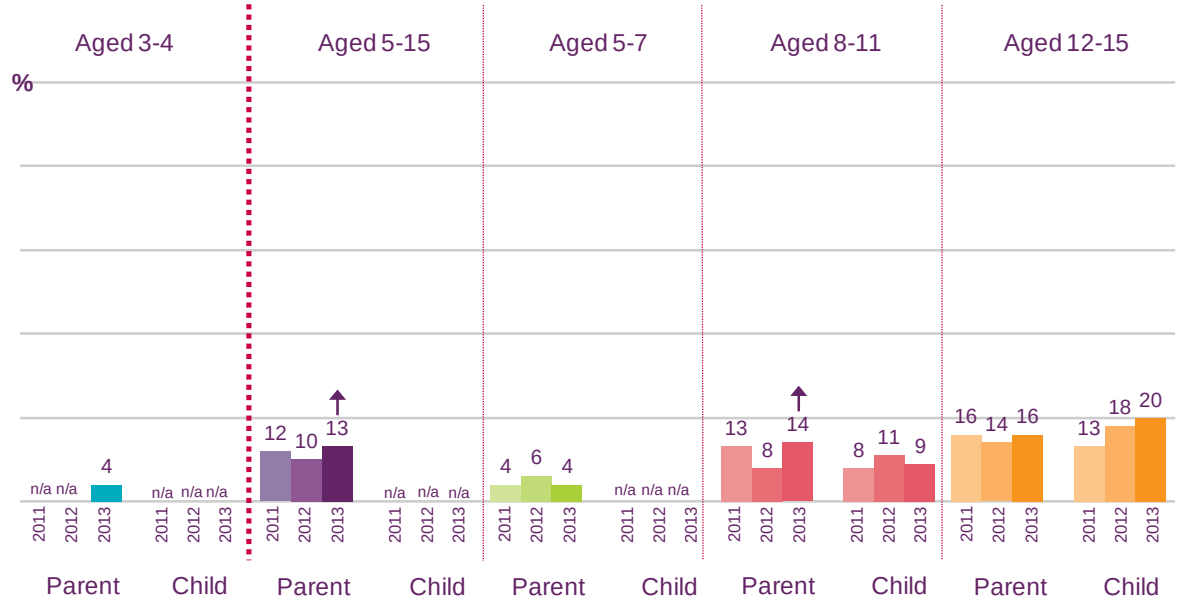
5.48 Girls aged 12-15 are more likely than boys to say they know of someone who has been bullied through a mobile phone (33% vs. 20%) and to say they have themselves experienced bullying in this way (12% vs. 3%). Girls aged 12-15 are also more likely than boys to say they feel under pressure to appear popular or attractive online (6% vs. 1%) and to have experienced gossip being spread about them online or through texts (17% vs. 10%).

5.49 One in five 12-15s say they have seen something online in the past year that is worrying, nasty or offensive.

5.50 Figure 11 compares the parent's estimate to the child's claimed experience of having seen something online in the past year that is worrying, nasty or offensive. There has been an overall rise in the parent's estimate, driven by an increase in parents of 8-11s estimating that they will have come into contact with some potentially inappropriate content. This increase is not reflected in the child's reported experience.

5.51 Only a very small number of 8-15s now say they would not tell someone if they found something online that was worrying, nasty or offensive (1% vs. 3% for 8-11s, and 4% vs. 8% for 12-15s).

Figure 11: Parent's estimate, and child's claimed experience, of having seen any online content in the last year that is considered worrying, nasty or offensive, by age: 2011–2013



QP59/ QC34 – In the last year, do you think your child has seen anything online that is worrying, nasty or offensive in some way?/ And in the last year, have you seen anything online that you found worrying, nasty or offensive in some way? (Prompted responses, single coded)
Base: Parents of children aged 3-15 whose child uses the internet at home/ Children aged 8-15 who use the internet at home or anywhere else (219 aged 3-4 in 2013, 1421 aged 5-15 in 2011, 1424 aged 5-15 in 2012, 1426 aged 5-15 in 2013, 396 aged 5-7 in 2011, 376 aged 5-7 in 2012, 381 aged 5-7 in 2013, 496 aged 8-11 in 2011, 495 aged 8-11 in 2012, 554 aged 8-11 in 2013, 529 aged 12-15 in 2011, 553 aged 12-15 in 2012, 565 aged 12-15 in 2013 – Significance testing shows any difference between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Parental concerns

Parental concerns and attitudes to the internet

5.52 The 2012 qualitative study showed that parenting was perceived to be a constant challenge, characterised by the need to balance a number of often conflicting priorities such as:

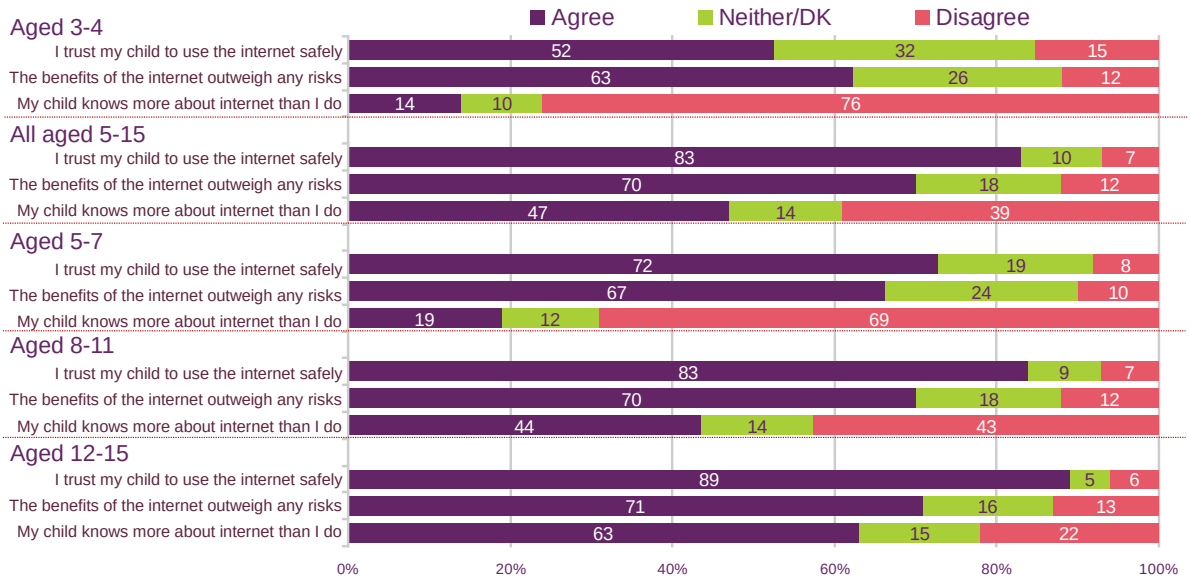
- Maintaining an open relationship with children but also setting boundaries;
- Allowing children freedom to explore but also protecting them from threats; and
- Providing children with access to benefits of technology and the internet specifically, but also protecting them from any negative effects and risks.

5.53 Managing children's use of the internet emerged spontaneously as a key part of the parenting balancing act, prior to any specific prompting about technology. It was one

of the primary aspects felt to distinguish modern parenting from the experience of previous generations. This lack of precedent, along with the rapidly changing nature of technology, meant parents were unclear what they needed to do to 'get it right'.

5.54 In the 2013 quantitative study, parents of children aged 3-15 who use the internet at home were asked about the extent to which they agreed or disagreed with a range of statements about their child's use of the internet. Figure 12 summarises these attitude statements by age for 2013.

Figure 12: Summary of parental agreement with attitudinal statements about the internet, by age: 2013



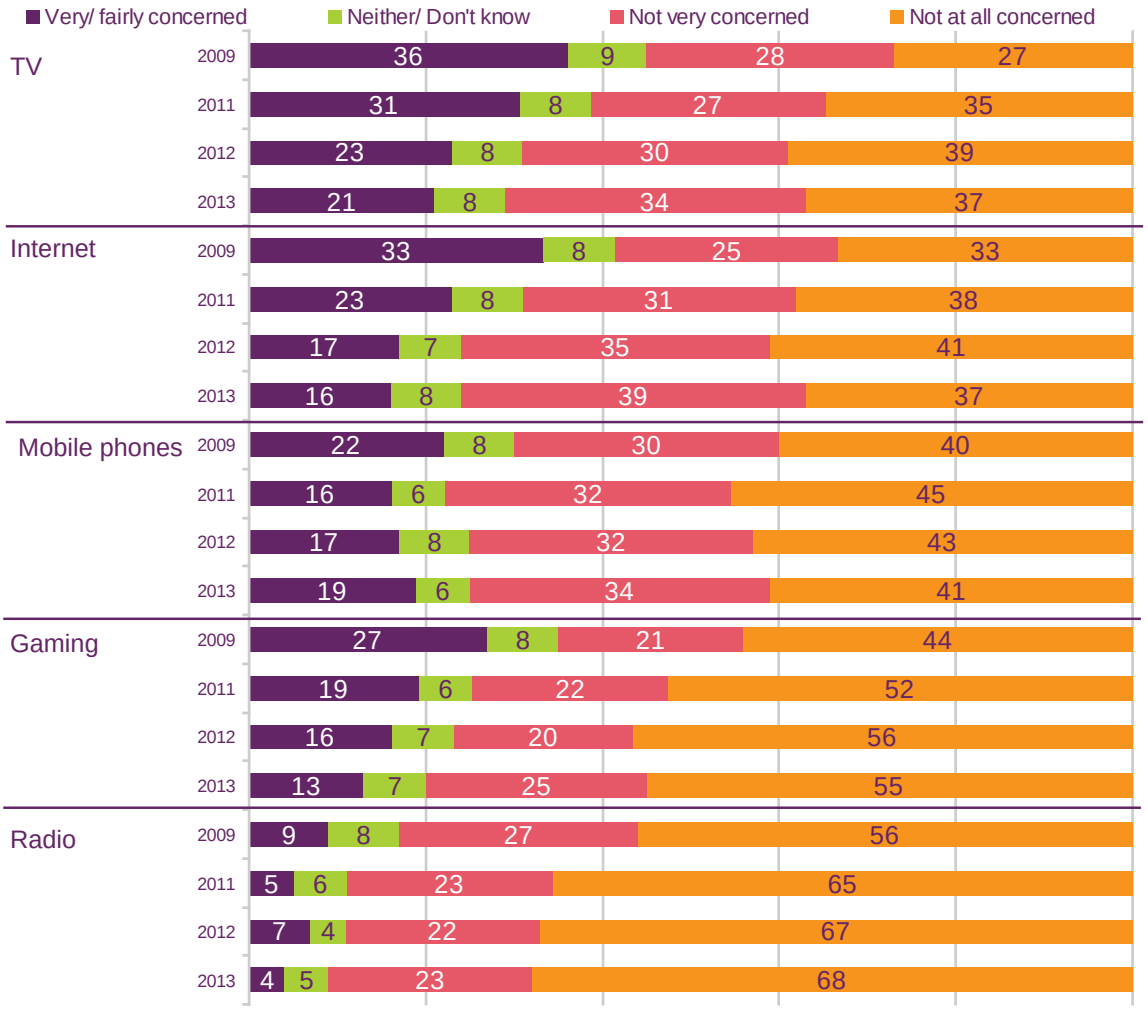
QP49A/ B/ C – Please tell me the extent to which you agree or disagree with these statements in relation to your child? (prompted responses, single coded)
Base: Parents of children who use the internet at home (219 aged 3-4 in 2013, 1426 aged 5-15 in 2013, 381 aged 5-7 in 2013, 497aged 8-11 in 2013, 548 aged 12-15 in 2013)
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

5.55 Most parents (83%) say that they trust their child to use the internet safely. The likelihood increases with the age of the child so that 52% of parents of 3-4s, 72% of parents of 5-7s, 83% of parents of 8-11s and 89% of parents 12-15s agree with the statement that they trust their child to use the internet safely. The majority of parents continue to feel that the benefits of the internet outweigh the risks.

5.56 However, close to half of parents say that their child knows more about the internet than they do, including one in seven (14%) parents of children aged 3-4. Compared to 2012, parents of 8-11s are now more likely to say this (44% vs. 35%) and the figure increase to 63% for parents of 12-15s.

5.57 Since 2009, parents overall are less likely to be concerned about television, online and gaming content, with the biggest decline in concern being for online and television content, as shown in Figure 13.

Figure 13: Parental concerns about media content, among parents of 5-15s using each media type: 2009, 2011–2013

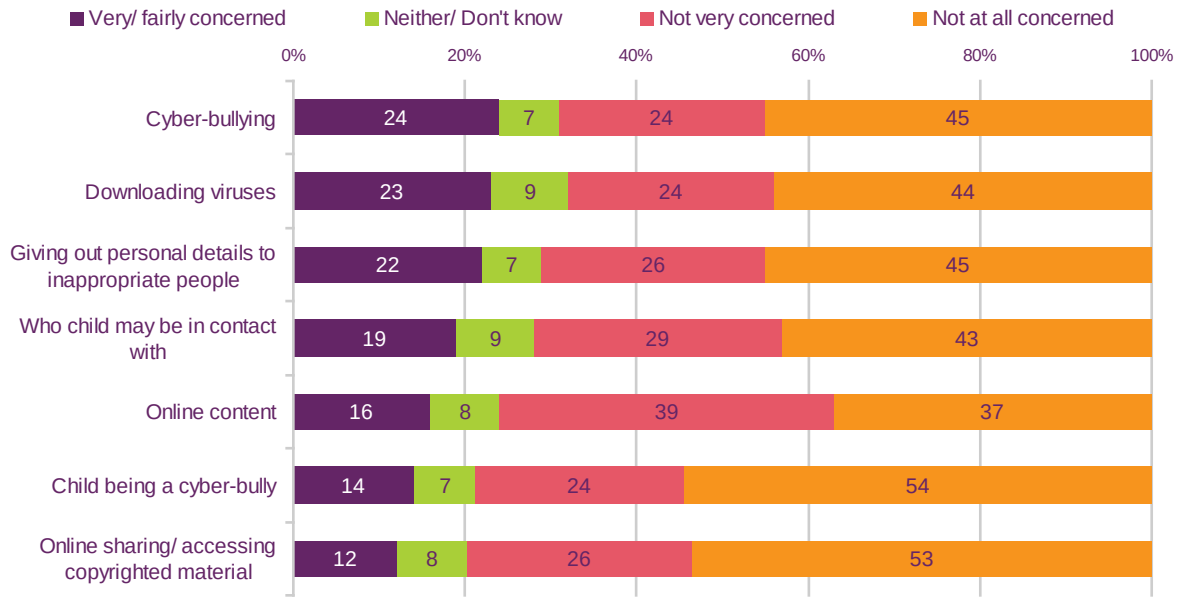


QP18A/ QP57A/ QP68A/QP86A/QP25A – Please tell me the extent to which you are concerned about these aspects of your child's TV viewing /internet use/ mobile phone use? (prompted responses, single coded)
Base: Parents of users of each media) aged 5-15 (VARIABLE BASE– significance testing show s any change between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

5.58 Figure 14 below summarises the various concerns that parents of 5-15s who use the internet at home were asked about. Among all parents, around one in four are concerned about their child being bullied (24%), downloading viruses (23%) or giving out personal details to inappropriate people (22%). One in five parents, or fewer, are concerned about who their child may be in contact with online (19%), the content of the websites their child visits (16%), their child potentially being a cyberbully (14%) or about any illegal online sharing or accessing of copyrighted material (12%).

5.59 Concerns about who the child is in contact with increase with the age of the child, with parents of 12-15s more likely to be concerned than parents of 8-11s (26% vs. 16%) and parents of 8-11s more likely to be concerned than parents of 5-7s (16% vs. 9%).

Figure 14: Parental concerns about aspects of their child's internet use among 5-15s: 2013



QP57A/C-H – Please tell me the extent to which you are concerned about these possible aspects of your child's internet use (prompted responses, single coded)
Base: Parents of children who use the internet at home (1426 aged 5-15 in 2013)
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

5.60 The 2012 qualitative study noted that most top-of-mind of potential concerns were not specifically risks related to inappropriate exposure to content or contact-related risks, which few parents felt their children had direct experience of and therefore tended to treat as hypothetical.

5.61 Instead, concerns tended to be focused on other issues and problems that parents were regularly facing related to their children's day-to-day internet usage. These included the struggle to achieve family time away from screen-based devices, the risk of less interest in physical and outdoor activities and a decline in perceived 'traditional' skills such as handwriting, spelling and the ability to communicate face-to-face.

5.62 However, when discussing online risks specifically, it was apparent the internet was felt both to create new risks and to transform traditional ones. New risks were perceived to arise from the unprecedented access to explicit material online and the growing area of user-created content, through social networking sites and video sharing sites like YouTube. Bullying and stranger danger were perceived to be transformed by the online environment into something far greater and more difficult to control.

5.63 Parents perceived there to be a hierarchy both in prevalence and seriousness of internet-related risks. 'Transactional' risks (e.g. getting viruses or running up bills) were perceived to be relatively commonplace but limited in their impact on the child's well being. Conversely, 'contact' risks (e.g. cyberbullying or grooming online) were expected to be relatively rare but considered the most serious in terms of impact or harm.

5.64 Both of these risks were more top-of-mind compared to 'content' risks (e.g. accidentally or deliberatively accessing unsuitable material). This was because content risks were neither seen as the most common or serious of risks.

5.65 However, a potential longer-term effect of exposure to inappropriate content was perceived to be desensitisation and inappropriate values with respect to relationships, sex and body image.

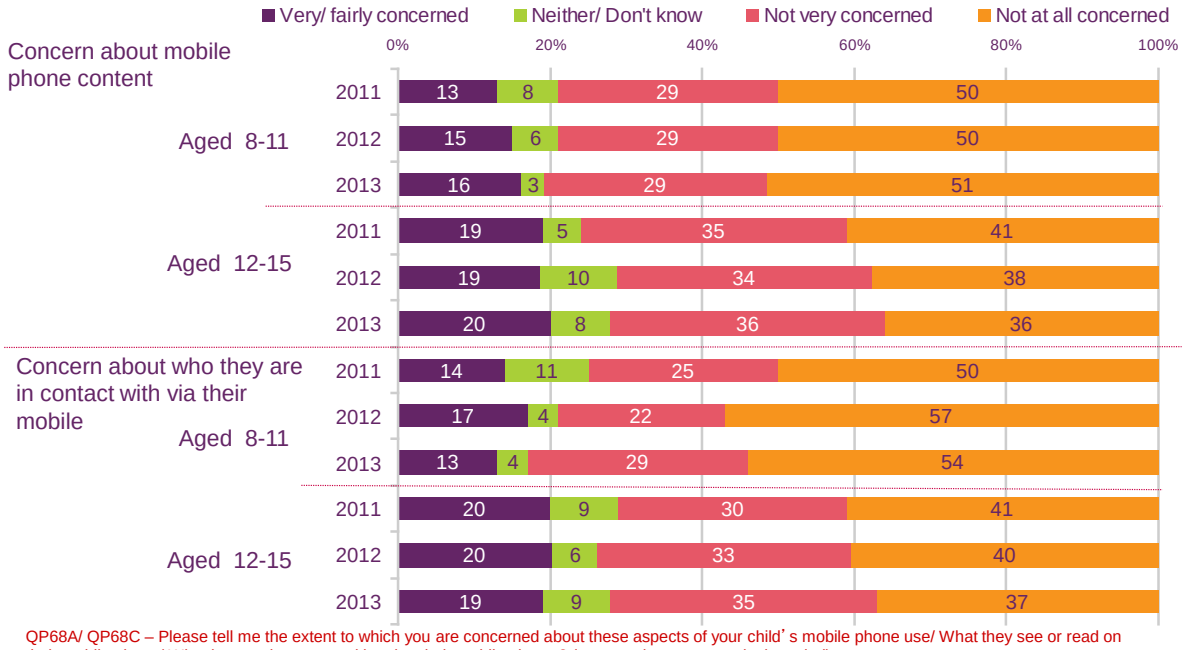
5.66 In addition, parents noted there was some convergence of content and contact risks seen in the areas of online gaming and social media, and this convergence was perceived to elevate the risk of serious potential harm for children.

Parental concerns about mobile phones

5.67 Turning to the 2013 quantitative research, figure 15 shows that concerns around 'contact' and 'content' via mobile phones is relatively low, 16% and 13% respectively for parents of 8-11s and 19% and 20% respectively for parents of 12-15s.

5.68 In 2013, parents of children aged 12-15 with a smartphone are no more likely than parents whose child has a non-smartphone to be concerned about both these aspects of their child's mobile phone use. This was not the case in 2012.

Figure 15: Parental concerns about mobile phone content and who their child is in contact with via their mobile, by age: 2011–2013



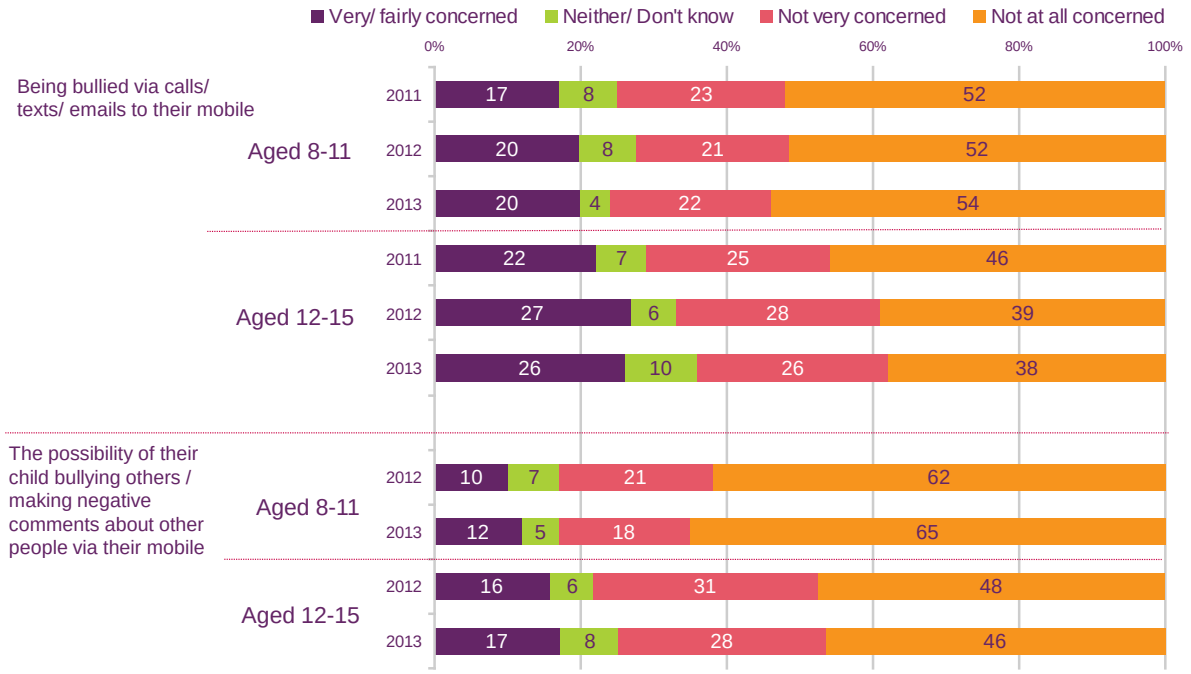
QP68A/ QP68C – Please tell me the extent to which you are concerned about these aspects of your child's mobile phone use/ What they see or read on their mobile phone/ Who they are in contact with using their mobile phone ? (prompted responses, single coded)
Base: Parents of children whose child has their own mobile phone (274 aged 8-11 in 2011, 238 aged 8-11 in 2012, 188aged 8-11 in 2013, 496 aged 12-15 in 2011, 493 aged 12-15 in 2012, 467 aged 12-15 in 2013). Significance testing shows any difference between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

5.69 Figure 16 shows that a fifth of parents of 8-11s (20%) and one in four parents of 12-15s (26%) say they are concerned about bullying via mobile phones.

5.70 One in eight parents (12%) of a child aged 8-11 and around one in six (17%) parents of a 12-15 year old say they are concerned about the possibility of their child bullying others or making negative comments about other people via their mobile phone. Parents of 12-15s are more likely to be concerned about their child being bullied through their mobile phone than about the possibility of their child bullying others in this way.

5.71 These concerns do not vary based on whether the child has a smartphone or a non-smartphone.

Figure 16: Parental concerns about their child being bullied via calls/texts/emails to the child's mobile phone, and the possibility of their child bullying others/making negative comments about other people via their mobile phone, by age: 2011–2013



QP68H/ QP68I – Please tell me the extent to which you are concerned about these aspects of your child's mobile phone use/ Being bullied via calls /texts/ emails/ messages to their mobile phone/ The possibility of them bullying others or making negative comments about other people via their mobile phone (prompted responses, single coded)
Base: Parents of children whose child has their own mobile phone (274 aged 8-11 in 2011, 238 aged 8-11 in 2012, 188aged 8-11 in 2013, 496 aged 12-15 in 2011, 493 aged 12-15 in 2012, 467 aged 12-15 in 2013). Significance testing shows any difference between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

5.72 A similar proportion of parents who are concerned about their child being bullied through their mobile phone are concerned about their child giving out personal details to inappropriate people (18% for 8-11s and 25% for 12-15s).

5.73 One in four parents of 8-11s with a smartphone (24%) are concerned about their child downloading malicious or bogus apps. One in five parents of 12-15s with a smartphone (19%) also have this concern.

5.74 Parents of children with a smartphone are as concerned about their child's use of location-based services, as they are about downloading malicious apps, with around one in five parents having this concern (21% for parents of 8-11s and 18% for parents of 12-15s).

5.75 As with other concerns regarding mobile phones, a majority of parents of children with smartphones are unconcerned about either of these measures.

Parental concerns about online gaming

5.76 The vast majority of parents of 5-15s say they are unconcerned about who their child is playing online games with through the games player.

5.77 Among parents of 3-4s, concerns about who their child is playing games with through the games player are at a comparable level to their concerns about gaming content; three in four of these parents (76%) are not at all concerned and less than one in 20 (3%) are concerned.

5.78 Parents of boys aged 12-15 are more likely to be concerned than parents of girls of this age (18% vs. 6%). Parents of 8-11s are less likely to say they are not at all concerned (58% vs. 68% in 2012).

5.79 One in six parents of children aged 5-15 (16%) are concerned overall about the cost of in-game purchases (for things like access to additional points/tokens/levels or for game upgrades).

5.80 As with some of the other mobile phone-related concerns, parental responses among parents of 3-4s are in line with those given by parents of 5-7s. One in ten parents are concerned (10%) and two in three (67%) are not at all concerned.

5.81 Parents of boys aged 8-11 and 12-15 are more likely than parents of girls in each age group to say they are concerned (24% vs.15% for 8-11s and 20% vs. 10% for 12-15s).

Section 6

Parental mediation strategies: take-up, awareness and confidence in parental controls

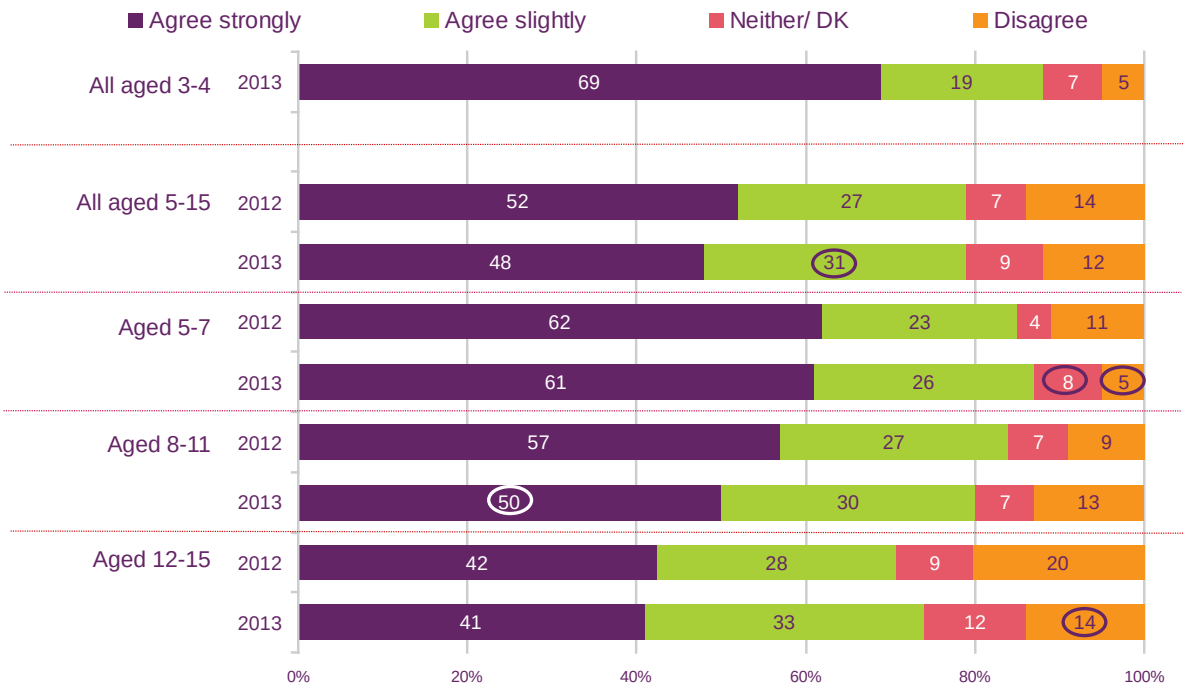
Key findings

- Parents of 5-15s use a combination of approaches to mediate their child's internet use, including: regularly talking to their children about staying safe online and having technical controls and rules about parental supervision. Eighty-five per cent of parents of 5-15s whose child ever goes online at home through a PC/laptop or netbook use at least one of these approaches.
- Seventy-nine per cent of parents of 5-15s who use the internet at home have spoken to their child about staying safe online and 45% of parents talk to their child about this at least once a month.
- Over half of parents have set rules around supervision of the internet which include regularly checking what children are doing online or only using when supervised.
- Over six in ten parents use some kind of technical mediation such as parental controls, safe search settings, You Tube safety Mode, time-limiting software or PIN/Passwords set on broadcasters' websites.
- Over four in ten parents of 5-15s say they have parental controls set on a PC, laptop or netbook. Forty per cent of parents of 3-4s have such controls in place. A majority of parents with these parental controls installed agree strongly that these controls are effective and that their child is safer as a result.
- Among parents whose child has a mobile phone that can be used to go online, four in ten parents of 12-15s (40%) and close to half of parents of 8-11s (47%) have applied filters to exclude websites aimed at over-18s.

Parents' confidence around keeping their child safe online

6.1 Figure 17 shows that the majority of parents of 5-15s agree that they feel they know enough to help their child to stay safe when they are online. Parents of younger children are more likely to agree strongly than parents of older children.

Figure 17: Parents who feel they know enough about how to help their child to stay safe online, by age: 2012–2013



QP49D –Please tell me the extent to which you agree or disagree with these statements in relation to your child - I feel I know enough to help my child to stay safe when they are online (prompted responses, single coded)
Base: Parents of children aged 5-15 whose child uses the internet at home (219 aged 3-4 in 2013,,424 aged 5-15 in 2012, 1426 aged 5-15 in 2013, 376 aged 5-7 in 2012, 381 aged 5-7 in 2013, 495 aged 8-11 in 2012, 497 aged 8-11 in 2013, 553 aged 12-15 in 2012, 548 aged 12-15 in 2013) - Significance testing shows any difference between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

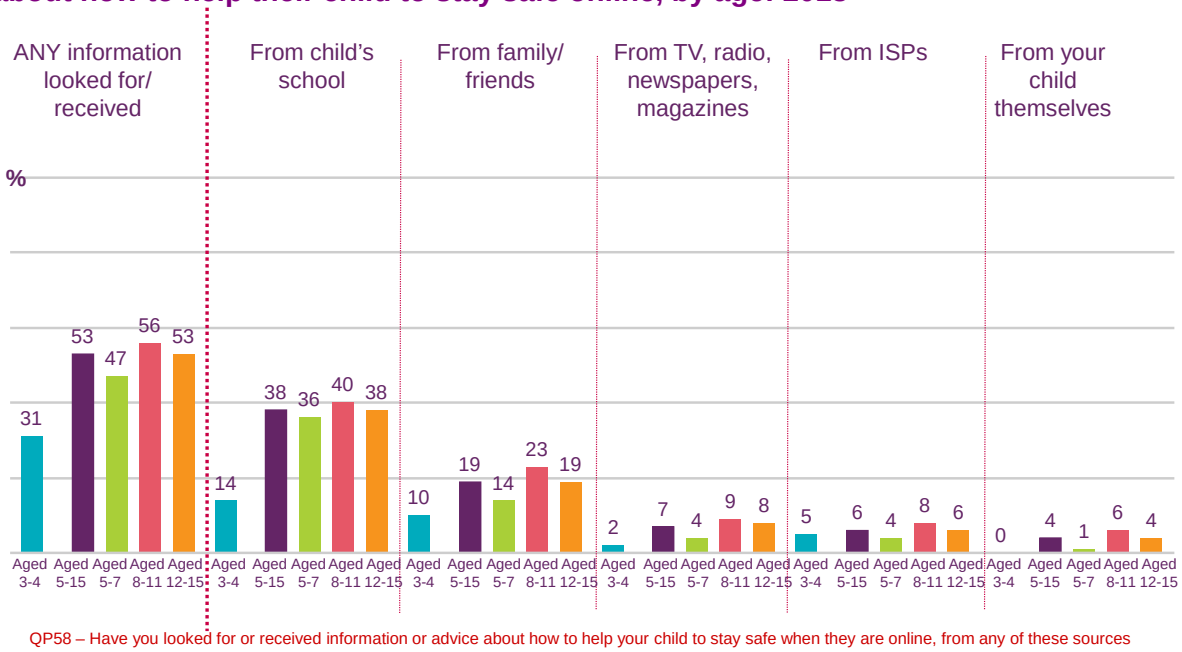
6.2 A majority of parents of children aged 5-15 (53%) have looked for or received information/advice from any source about how to help their child stay safe online. Figures 18 and 19 show the responses given by parents[33] when they were prompted with 14 possible sources, with the option of nominating other sources.

6.3 Among parents of 5-15s, the most popular source of information is the child's school. Information from family/friends is the next most common source of information named by a sizeable minority of parents (19% of all parents of 5-15s, rising to 23% among parents of 8-11s). Fewer than one in ten parents of 5-15s have looked for or received information from the media (TV/radio/newspapers/magazines) (7%) or from ISPs (6%). No other sources, (including special interest groups such as CEOP/GSO/UKCCIS) were used by more than one in 20 parents.[34] Four per cent of parents of 5-15s say they have received information from their child.

6.4 Figure 19 also shows that sources other than family, friends or the child themselves account for the majority of information received about how to help their child stay safe online – with these sources mostly consisting of information provided by the child's school.

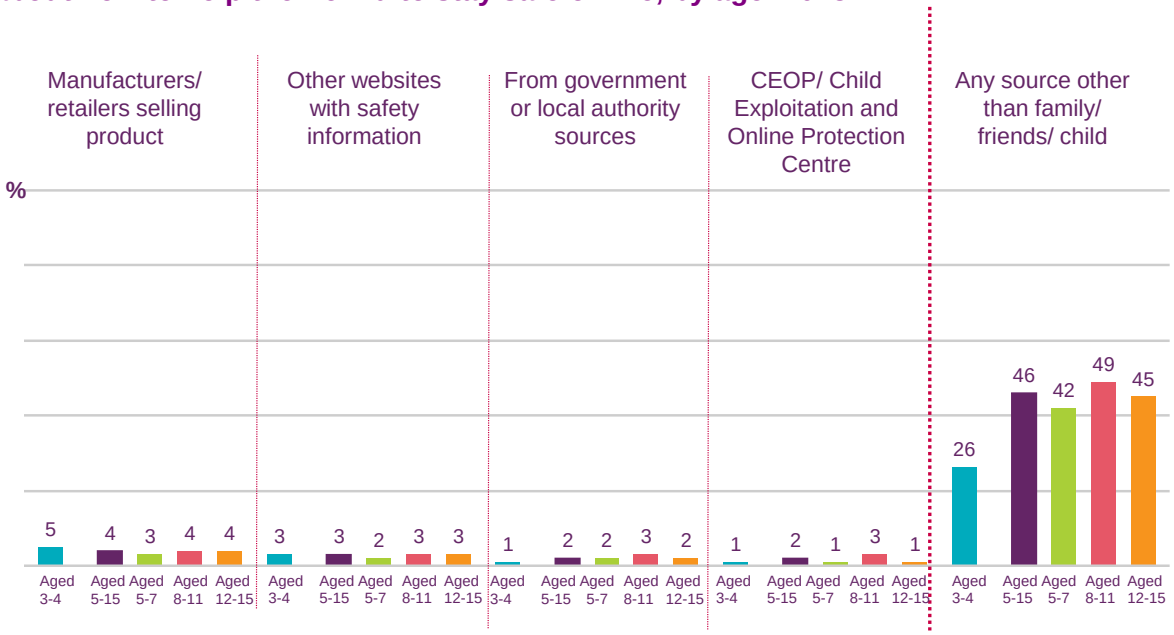
[33] Where more than 1% of parents gave that response.
[34] 2% of parents of 5-15s whose child goes online at home have sourced/received information from CEOP, as have 1% of parents from GSO and 1% of parents from UKCCIS.

Figure 18: Parents stating they have looked for or received any information or advice about how to help their child to stay safe online, by age: 2013



QP58 – Have you looked for or received information or advice about how to help your child to stay safe when they are online, from any of these sources or in any other way? (prompted responses, multi-coded) – only responses shown where>1% of all parents have given that answer
Base: Children aged 5-15 who use the internet at home (219 aged 3-4, 1426 aged 5-15, 381 aged 5-7, 497 aged 8-11, 548 aged 12-15)
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Figure 19: Parents stating they have looked for or received any information or advice about how to help their child to stay safe online, by age: 2013



QP58 – Have you looked for or received information or advice about how to help your child to stay safe when they are online, from any of these sources or in any other way? (prompted responses, multi-coded) – only responses shown where>1% of all parents have given that answer
Base: Children aged 5-15 who use the internet at home (219 aged 3-4 1426 aged 5-15, 381 aged 5-7, 497 aged 8-11, 548 aged 12-15)
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Parental mediation strategies

6.5 Parents of 5-15s use a combination of approaches to mediate their child's internet use, including:

- regularly talking to their children about staying safe online;
- mediation through technical tools;
- having rules relating to parental supervision.

6.6 Figure 20 shows the relationship between three main types of mediation that parents may choose to use at home with regard to their child's use of the internet (through a PC/laptop/netbook) and shows the interplay of supportive guidance (talking to their child about staying safe online at least monthly), mediation through technical tools[35] and rules or restrictions relating specifically to parental supervision.[36]

6.7 Eighty-five per cent of parents of 5-15s whose child ever goes online at home through a PC/laptop or netbook use at least one of these approaches. One in five parents of 5-15s (20%) use all three of these types of mediation; they use technical mediation, have rules relating to parental supervision and have talked to their child at least monthly about staying safe online. This is more likely among parents of 8-11s (25%) than parents of 3-4s (8%), 5-7s (14%) or 12-15s (19%).

6.8 Thirty-five per cent of parents use two of these approaches and 30% use only one. Fifteen per cent do none of the things asked about and this is higher for 12-15s (22%) than for 5-7s (11%) and 8-11s (9%).

6.9 Fewer than one in ten parents of 3-4s (8%) use all three approaches, while close to one in five (18%) do none of them and this is higher than for 5-7s (11%) and 8-11s (9%). These incidences are all unchanged since 2012.

6.10 Seventeen per cent have rules relating to parental supervision and use technical mediation, but do not talk to their child at least monthly about staying safe online, with this being more likely for 5-7s (22%) than for 12-15s (13%). One in five parents of 3-4s (19%) also use this approach.

6.11 One in 20 parents of 5-15s (6%) *only* talk to their child at least monthly about staying safe online; higher for 12-15s (10%) than for 3-4s (2%), 5-7s (2%) or 8-11s (5%). Only having rules relating to parental supervision is higher for 3-4s (22%) and 5-7s (20%) than for 8-11s (11%) or 12-15s (6%). Only relying on technical mediation is more likely for 3-4s (23%) and 5-7s (17%) than for 12-15s (11%).

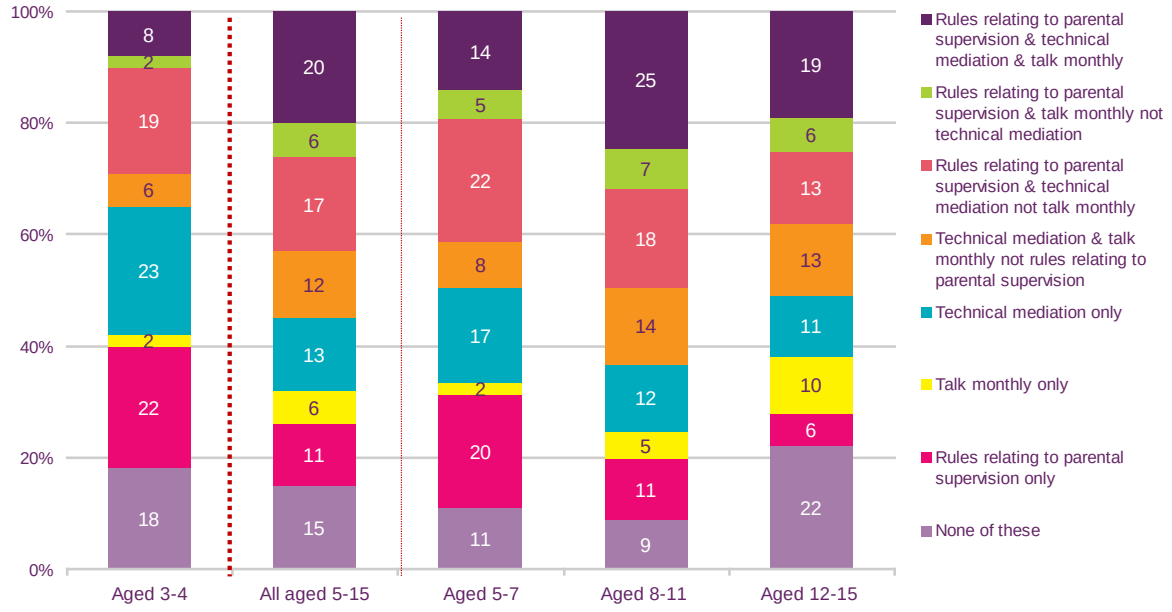
6.12 It is important to note that while 15% of parents fall into the category of 'none of these', around six in ten of these (9%) *do* talk to their child about staying safe online, but they do so less frequently than monthly. Therefore, the remaining 6% of parents have never spoken to their child about staying safe online, do not have rules about

[35] Use at least one of the five types of technical mediation tools shown Figure 36 – Safe search settings, parental controls, YouTube safety mode, software to limit the time spent online or PIN/passwords set up on broadcasters' websites.

[36] These relate to the two specific online rules: "Regularly check what they are doing online" and "can only use when supervised and not on their own".

parental supervision or do not have technical mediation in place. This incidence does not vary by age, gender or by household socio-economic group.

Figure 20: Combinations of online mediation strategies used by parents of 5-15s where a child uses a PC/laptop/netbook to go online at home, by age: 2013



Base: Parents of children aged 5-15 whose child ever uses a PC/ laptop/ netbook to go online at home (185 aged 3-4, 1354 aged 5-15, 362 aged 5-7, 471 aged 8-11, 521 aged 12-15)
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

6.13 The 2012 qualitative study suggested that the approach parents took to mediating in this area was generally consistent with their overall parenting style, and here respondents typically spoke of their aim to balance rules and boundaries with trust and freedom. Instilling the right values and habits in their children was also seen to be critical.

6.14 Overall, technical tools were viewed as a supplement to, rather than replacement for, hands-on parenting. Supervision and other forms of parental mediation were felt still to be needed to prevent all of the day-to-day issues as well as risks emanating from children's internet usage.

6.15 As in quantitative research, almost all stated they were doing something specific to mediate their children's use of the internet, and most claimed to be using a combination of approaches, such as:

- Rules around limiting access – e.g. setting time limits; only allowing their child online at certain times; banning access to certain sites; banning certain activities.
- Supervision of activities – e.g. only allowing internet in common view; checking what children are doing.
- Monitoring of activities – e.g. checking child's internet history; vetting social network friends; monitoring social network activity as a 'friend'; knowing child's passwords.

- Communication about staying safe online – e.g. a formal sit-down conversation and/or more informal ongoing communication; schools also play an important role here.

- Some were also using parental controls or other technical tools (e.g. safe searches, safe modes on websites).

Parental rules

6.16 The majority of parents of children (about 8 in 10) aged 3-15 have rules and restrictions in place for their child's use of mobile phones, gaming and the internet.

Parental rules for mobile phones

6.17 Figure 21 shows that most parents whose child has their own mobile phone have put in place at least one of the rules that was asked about. Many of the rules and restrictions for mobile phone use relate to the cost associated with using the phone rather than the possibility of encountering inappropriate or potentially harmful content.

6.18 Rules about mobile phone use are as likely for 12-15s as they are for 8-11s (71% vs. 73%). There are, however, four rules that are more likely among parents of 8-11s whose child has their own mobile phone, compared to parents of 12-15s: regularly check what they are doing with the phone (27% vs. 14%); only calls/texts to an agreed list of people (25% vs. 7%); use only to make/receive voice calls or send texts, and nothing else (19% vs. 8%); and no going online (13% vs. 8%).

6.19 There is only one rule that is more likely among parents of 12-15s compared to 8-11s: that the child is responsible for paying for top-ups/bills (16% vs. 8%).

6.20 While the overall incidence of rules is no different among parents of 12-15s with a smartphone than among parents of children with a non-smartphone (70% and 72% respectively), those aged 12-15 with a non-smartphone are more likely to have the rule about limiting how often credit can be put on the phone (44% vs. 30%) and only making/receiving calls or texts and nothing else (19% vs. 4%).

6.21 Parents of 12-15s with a smartphone are more likely than those with a non-smartphone to have the rule regarding regularly checking what they are doing with the phone (18% vs. 4%) and about only visiting certain websites on the phone (6% vs. 0%).

Figure 21: Parental rules for mobile phones, by age: 2013

	Aged 8-11	Aged 12-15
Any rules or restrictions	73%	71%
Limit how often credit can be put on the phone	38%	34%
No calls to premium rate numbers	24%	27%
No texts to premium rate numbers	23%	26%
Regularly check what they are doing with the phone	27%	14%
Child is responsible for paying top-ups/ bills	8%	16%
Only calls/ texts to an agreed list of people	25%	7%
Only to make/ receive voice calls or send texts, nothing else	19%	8%
No going online/ internet sites/ no WAP browsing	13%	8%
No downloading of apps/ applications onto the phone	12%	8%
Can only visit certain websites on the phone	6%	5%

QP67– Do you have any of these rules or restrictions about the use that your child makes of his/ her mobile phone ? (prompted responses, multi-coded)
Base: Parents of children aged 5-15 whose child has their own mobile phone (188 aged 8-11, 467 aged 12-15). Significance testing indicates any differences between 2012 and 2013.
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Parental rules about playing games

6.22 Most parents whose child plays games on a gaming device[37] say that they have rules or restrictions about the games their child plays. Figure 22 shows that rules are more likely to be in place for children aged 5-7 (86%) and 8-11 (81%), than for those aged 12-15 (58%). Close to nine in ten parents of 3-4s whose child plays games on a gaming device also have rules in place (88%).

6.23 Each individual rule is also less likely to be in place for 12-15s than for 3-4s, 5-7s or 8-11s.

6.24 More than half of parents of 3-4s, 5-7s and 8-11s have rules restricting the games played to those with an appropriate age rating (56%, 62% and 56% respectively), but this is less common among parents of 12-15s (34%).

6.25 Rules regarding the type of content of the games played (i.e. no games with violence or drug use or nudity/sexual content) are broadly comparable for parents of 3-4s, 5-7s and 8-11s and are considerably lower among parents of 12-15s. Girls aged 12-15 are more likely than boys to have rules about no online game playing (11% vs. 3%).

[37] This could be a fixed or portable games console/computer/mobile phone or portable media player.

Figure 22: Parental rules for gaming, by age: 2013

	Aged 3-4	Aged 5-15	Aged 5-7	Aged 8-11	Aged 12-15
Any rules or restrictions	88%	74%	86%	81%	58%
Only games with appropriate age rating	56%	50%	62%	56%	34%
No games after a certain time	35%	34%	40%	39%	25%
Regularly check on what they're playing	35%	32%	38%	39%	21%
No games with violence	35%	32%	40%	39%	19%
No games with drug use	34%	32%	40%	37%	20%
No games with nudity/ sexual content	33%	32%	39%	37%	20%
No games with swearing/ bad language	34%	31%	40%	37%	19%
No online game playing	22%	15%	24%	18%	7%
No online game playing with people they don't already know	15%	14%	19%	15%	8%
No online chat or messaging (added in 2013)	18%	12%	18%	16%	5%
Can only play when supervised/ not on their own	33%	11%	21%	11%	3%
Only a game that an adult or parent has played/ tried first	19%	10%	16%	12%	3%

QP77 - Do you have any of these rules or restrictions about the games that your child plays at home – whether on a games console, a computer or any other device? (prompted responses, multi-coded)
Base: Parents of children aged 5-15 whose child ever plays games at home on any type of game playing device (xxx aged 3-4, 1486 aged 5-15, 447 aged 5-7, 535 aged 8-11, 504 aged 12-15). Significance testing indicates any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Parental rules about the internet

6.26 Four in five parents of children aged 5-15 who use the internet at home (79%) say they have rules in place about the internet. As shown in Figure 23, the younger the child, the more likely the incidence of having rules about the internet: 5-7 (92%), 8-11 (86%), 12-15 (65%). However, the incidence of parents of 3-4s having rules in place about their child's internet use is lower than among parents of 5-7s (84% vs. 92%).

6.27 No single online rule is in place among the majority of parents of 3-4s. A sizeable minority of parents of 3-4s who go online at home have a rule about only visiting children's websites (44%) or about using the internet only when supervised/not on their own (42%).

6.28 There is no single rule in place for a majority of 5-7 year old internet users. Forty-four per cent of parents of 5-7s say they regularly check what their child is doing online, or have a rule about visiting children's websites only (44%). Around one in three parents say their child can go online only when supervised, and not on their own (37%) and cannot go online after a certain time (33%).

6.29 The rule relating to the parent regularly checking what their child is doing online is in place among half of all parents of 8-11s (51%). There are no other rules in place among the majority of parents of 8-11s. Parents of 8-11s are more likely than parents of 5-7s and 12-15s to have rules in place about no purchasing from websites (34% for 8-11s vs. 23% for 5-7s and 24% for 12-15s) and no social networking sites (28% for 8-11s vs. 19% for 5-7s and 9% for 12-15s).

6.30 There is no single rule in place for the majority of 12-15s who go online, and no single rule is more likely to be in place for 12-15s compared to younger children.

Figure 23: Parental rules for the internet, by age: 2013

	Aged 3-4	Aged 5-15	Aged 5-7	Aged 8-11	Aged 12-15
Any rules or restrictions	84%	**79%**	92%	86%	65%
Regularly check what they're doing online	25%	**45%**	44%	51%	41%
No internet after a certain time	28%	**32%**	33%	36%	28%
No purchasing from websites	10%	**27%**	23%	34%	24%
Only allowed to use the internet for a certain amount of time	13%	**21%**	23%	28%	13%
Only children's websites	44%	**19% ↓(-4)**	44% ↓ **(-9)**	22% ↓ **(-8)**	4%
Can only use when supervised/ not on their own	42%	**19%**	37%	22%	7%
No social networking websites	9%	**18%**	19% ↓ **(-9)**	28%	9% ↑ **(+4)**
PIN/ Password required to enter websites unless already approved	14%	**15%**	17%	18%	11%
Only talk/ chat with friends/ people they already know	2%	**13%**	13%	18%	10% ↓ **(-5)**
No Instant Messaging/ MSN	5%	**11%**	17%	17%	3%
Only websites stored in their Favourites list	10%	**9%**	12%	12%	4%
Only use for homework	0%	**5% ↓ (-2)**	5%	7%	3%

QP29 Do you have any of these rules or restrictions about the access that your child has to the internet on any device? (prompted responses, multi-coded)
Base: Parents of children aged 3-15 whose child uses the internet at home (219 aged 3-4, 1426 aged 5-15, 381 aged 5-7, 497 aged 8-11, 548 aged 12-15). Significance testing shows any difference between 2012 and 2013.
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Rules relating to parental supervision of the internet

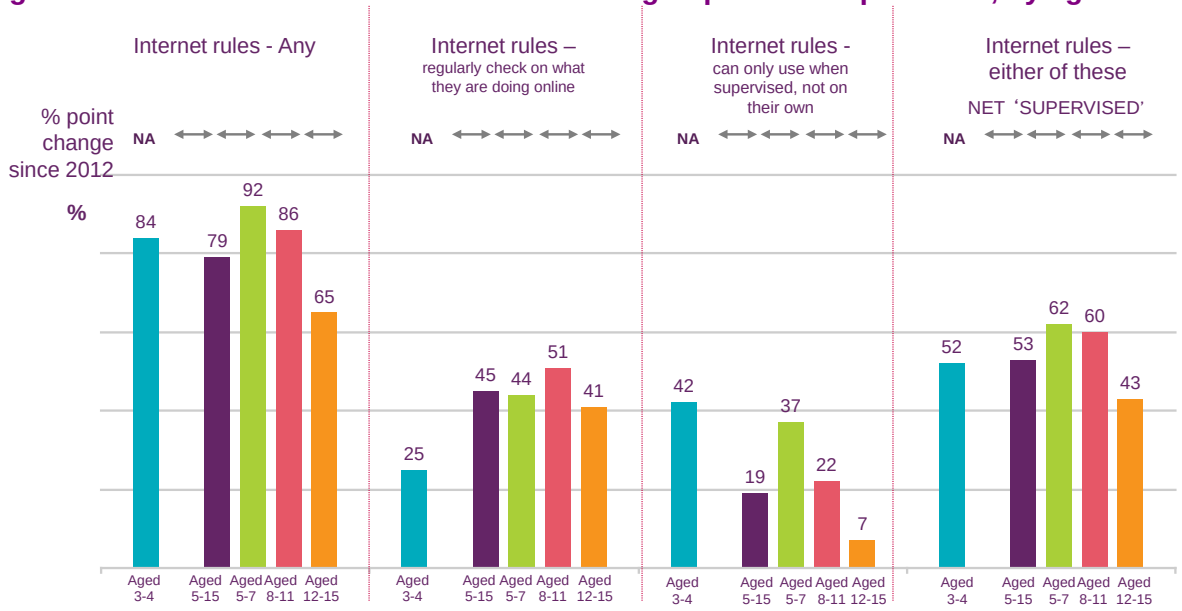
6.31 Figure 24 shows that just under half (45%) of all parents of 5-15s say they regularly check what their child is doing online. One in four parents of 3-4s also regularly check what their child is doing (25%).

6.32 The rule regarding children using the internet only when supervised and not on their own is in place for one in five 5-15s (19%) and decreases with age, with one in three (37%) parents of 5-7s having this rule, compared to 22% of 8-11s and around one in twenty 12-15s (7%). More than four in ten parents of 3-4s say their child can go online only when supervised (42%).

6.33 When the responses of parent who have either of these rules are combined, more than half of parents of 5-15s (53%) actively supervise their child in some way when online, with parents of 5-7s (62%) and 8-11s (60%) being more likely to do so than parents of 12-15s (42%).

6.34 When we add to this figure the responses of parents who have broader internet rules in place to manage potential content and contact risks, over six in ten parents (63%) have a combination of such rules in place.

Figure 24: Internet rules and restrictions relating to parental supervision, by age: 2013



QP29 Do you have any of these rules or restrictions about the access that your child has to the internet on any device? (prompted responses, multi-coded)
Base: Parents of children aged 3-15 whose child uses the internet at home (219 aged 3-4, 1426 aged 5-15, 381 aged 5-7, 497 aged 8-11, 548 aged 12-15).
Significance testing shows any difference between 2012 and 2013.
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Parental controls

Awareness and use of parental controls

6.35 The 2012 qualitative research found different levels of awareness and understanding of parental controls:

- Those with reasonable awareness of the different options, although even they did not necessarily know about all of the possible features.
- Those who had basic awareness of the existence of parental controls but lacked understanding of how they work or the different options that are available.
- Those who had never heard of internet parental controls or fundamentally misunderstood their nature.

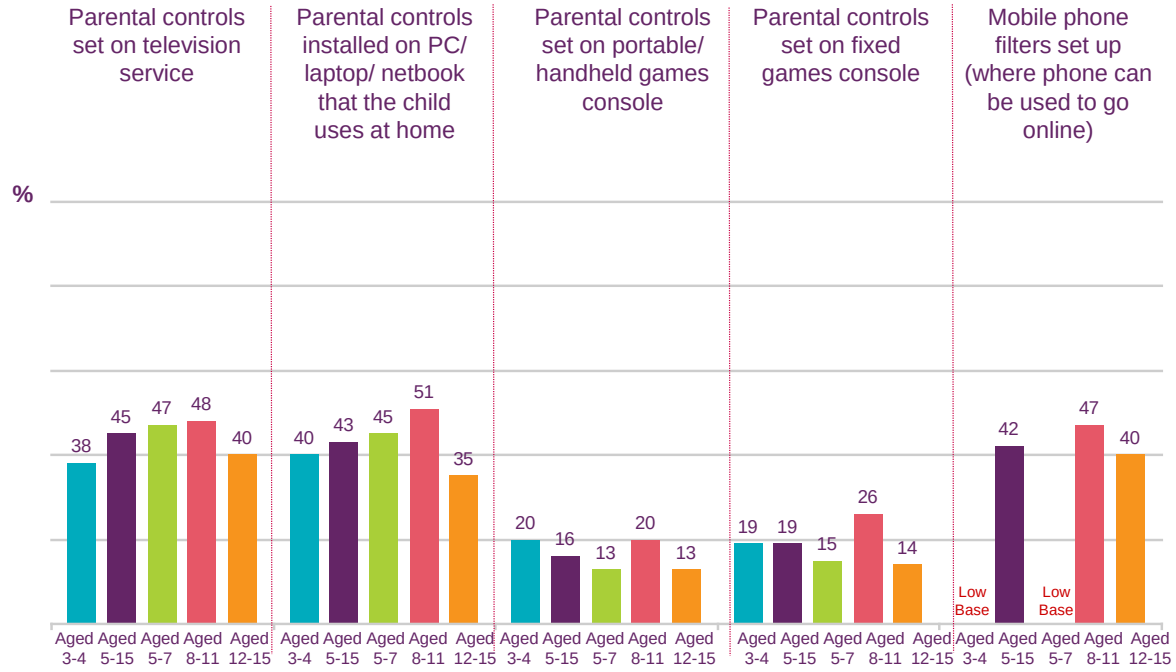
6.36 This indicates that understanding of parental controls is a somewhat 'grey area' and that even those who have some level of awareness also have gaps in their understanding. In general, more knowledgeable parents were more likely to have parental controls in place.

6.37 Figure 25 below gives a summary of the parental controls in place across TV, home PC/laptop/netbook, games consoles and mobile phone.

6.38 Four in ten parents have any of the four specific types of online controls installed on their computer at home, with this being more likely for 5-7s (45%) and 8-11s (51%) than for 12-15s (35%). Parents of 3-4s are as likely as parents of 5-7s to have controls in place (40% vs. 45%).

6.39 Figure 25 also shows that close to half of parents of 8-11s (47%) and four in ten parents of 12-15s (40%) say that their child's phone is limited to exclude these websites.

Figure 25: Summary of parental controls in place, by platform: 2013



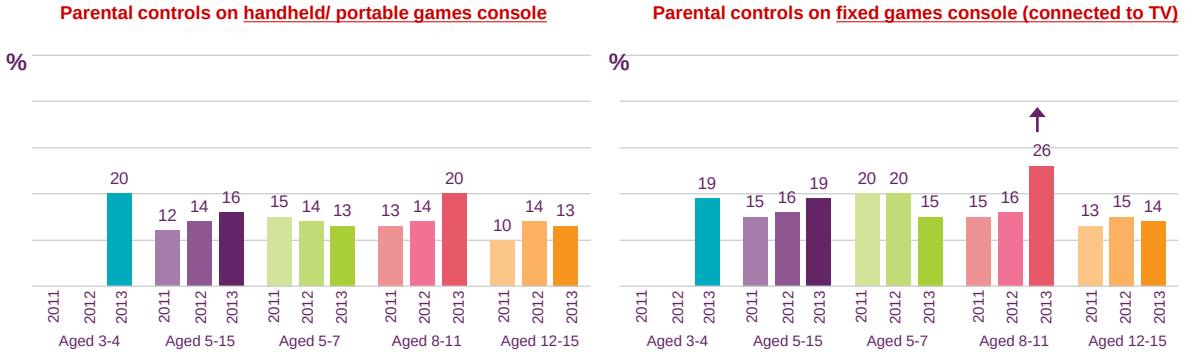
QP13/ QP30/ QP80/ QP81/ QP70 - Does your television service have any parental controls set to stop certain programmes, films or channels being viewed on your TV, until a PIN or password is entered/ Do you have any of these types of 'parental controls' loaded or put into place and working on the PC/ laptop/netbook that your child uses at home to prevent them viewing certain types of website/ Are there any parental controls set on the handheld games console?/ Are there any parental controls set on the games console that is connected to a TV?/ Is access to the internet on your child's phone limited to exclude websites that are aimed at people aged 18 and over?
Base: Parents of children aged 5-15 who watch TV at home/ Parents whose child aged 5-15 uses a PC/ laptop or netbook to go online at home/ Parents of children aged 5-15 with a portable games console/ Parents of children aged 5-15 with a fixed games console/ Parents of 5-15s with a mobile phone that can be used to go online
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

6.40 Controls are much less likely to be in place on handheld/portable games consoles (16%), or on fixed consoles (19%). Children aged 8-11 are more likely than 5-7s (15%) or 12-15s (14%) to have controls in place on a fixed games console (26%).

6.41 As shown in Figure 26, among 5-15s around one in six handheld/portable games consoles (16%) and one in five fixed games consoles (19%) have parental controls. In 2013, controls on fixed games consoles are more likely for 8-11s (26%) than for 5-7s (15%) or 12-15s (14%). A similar proportion of 3-4s have controls on a handheld games player (20%) as have controls on a fixed games console (19%).

6.42 In 2013, controls are more likely on fixed games consoles for boys aged 12-15 than for girls (18% vs. 9%). Compared to 2012, parents of 8-11s are more likely to have controls on fixed games consoles (26% vs. 16%).

Figure 26: Use of parental controls on games consoles, by age: 2011–2013



QP80/81– Are there any parental controls set on the handheld games console? / Are there any parental controls set on the games console that is connected to a TV? (spontaneous responses, single coded)
Base: Parents of children aged 5-15 with a portable games console (207aged 3-4 in 2013,1166 aged 5-15 in 2011, 1085 aged 5-15 in 2012, 899 aged 5-15 in 2013, 382 aged 5-7 in 2011, 397 aged 5-7 in 2012, 282 aged 5-7 in 2013, 454 aged 8-11 in 2011, 388 aged 8-11in 2012, 358 aged 8-11 in 2013, 330 aged 12-15 in 2011, 300 aged 12-15 in 2012, 259 aged 12-15 in 2013)/ Parents of children aged 5-15 with a fixed games console (169 aged 3-4, 1271 aged 5-15 in 2011, 1254 aged 5-15 in 2012, 1071 aged 5-15 in 2013, 366 aged 5-7 in 2011, 390 aged 5-7 in 2012, 290 aged 5-7 in 2013, 459 aged 8-11 in 2011, 440 aged 8-11 in 2012, 401 aged 8-11 in 2013, 446 aged 12-15 in 2011, 424 aged 12-15 in 2012, 380 aged 12-15 in 2013). Significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

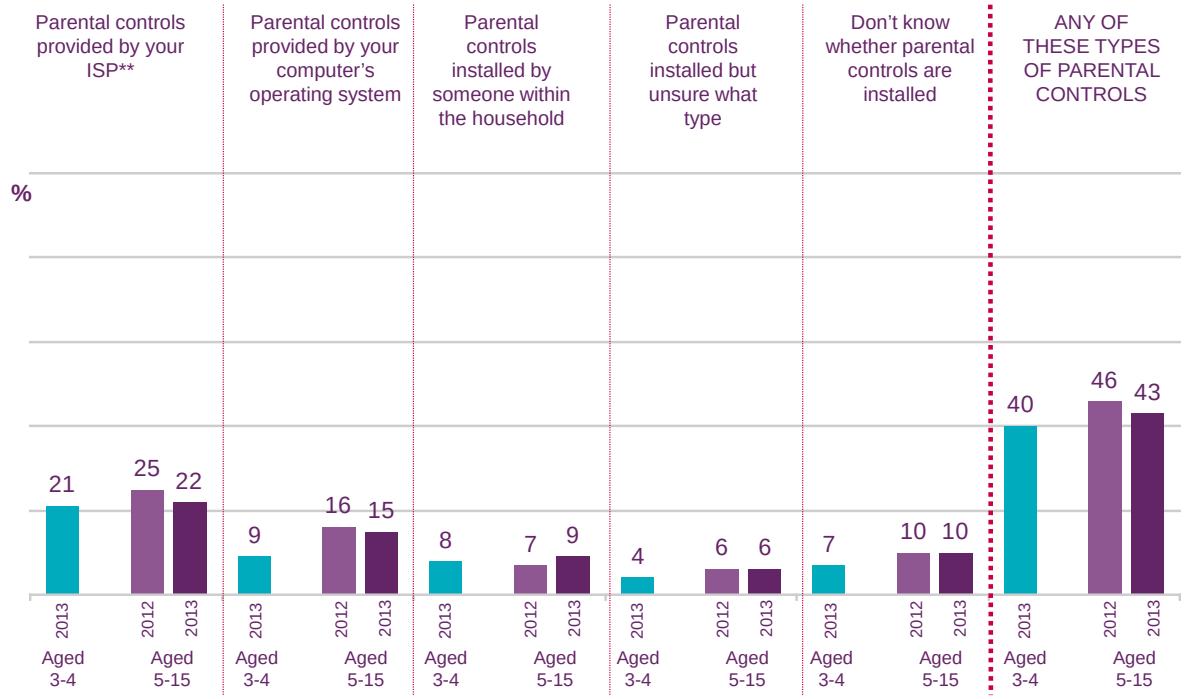
Types of parental controls installed on a PC/laptop/netbook

6.43 Parents whose child uses either a PC/laptop or a netbook to go online at home were prompted with four specific types of online parental controls and asked whether these were installed on the PC/laptop/netbook that their child uses:

- parental controls in place that were provided by their ISP[38];
- parental controls provided by the computer's operating system (e.g. Windows, Mac etc.);
- parental controls that someone in the household had installed or downloaded onto the computer, either free or paid for (e.g. Net Nanny, Open DNS, Family Shield);
- parental controls installed, but unsure of the specific type of controls.

[38] ISP-provided controls could include any of the following: network level filtering e.g. 'Homesafe' from TalkTalk or software - like McAfee Family Protection - provided by ISPs for people to install on their computers.

Figure 27: Types of parental controls installed on the PC/laptop/netbook the child uses at home, by age: 2012–2013



QP30 – Do you have any of these types of parental controls loaded or put in place and working on the PC/ laptop/ netbook that your child uses at home to prevent them viewing certain types of website? (prompted responses, multi-coded) **ISP-provided controls could include any of the following: network level filtering e.g. 'Homesafe' from TalkTalk or software - like McAfee Family Protection - provided by ISPs for people to install on their computers
Base: Parents whose child uses a PC, laptop or netbook to go online at home (1405 aged 5-15 in 2012, 1354 aged 5-15 in 2013, 185 aged 3-4 in 2013) - Significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

6.44 Figure 27 shows that close to half of parents of 5-15s (43%) have any of these types of parental controls installed on their PC/laptop/netbook. Parents of 5-7s (45%) and 8-11s (51%) are more likely than parents of 12-15s (35%) to have any of them in place. Any of these types of control are in place among four in ten parents of 3-4s who go online at home through a PC/laptop or netbook (40%).

6.45 The most commonly installed parental controls among parents of 5-15s who use a PC, laptop or netbook to go online at home were those provided by their ISP, with one in five (22%) claiming to have this. ISP-provided controls could include any of the following: network level filtering e.g. 'Homesafe' from TalkTalk or software - like McAfee Family Protection - provided by ISPs for people to install on their computers..

6.46 Parental controls provided by the computer's operating system (e.g. Windows, Mac) are the next most popular type of parental control, with 15% of parents of 5-15s having these installed.

6.47 Around one in ten parents (9%) have parental controls that someone in the household had installed or downloaded onto the computer, either free or paid for (e.g. Net Nanny, Open DNS, Family Shield).

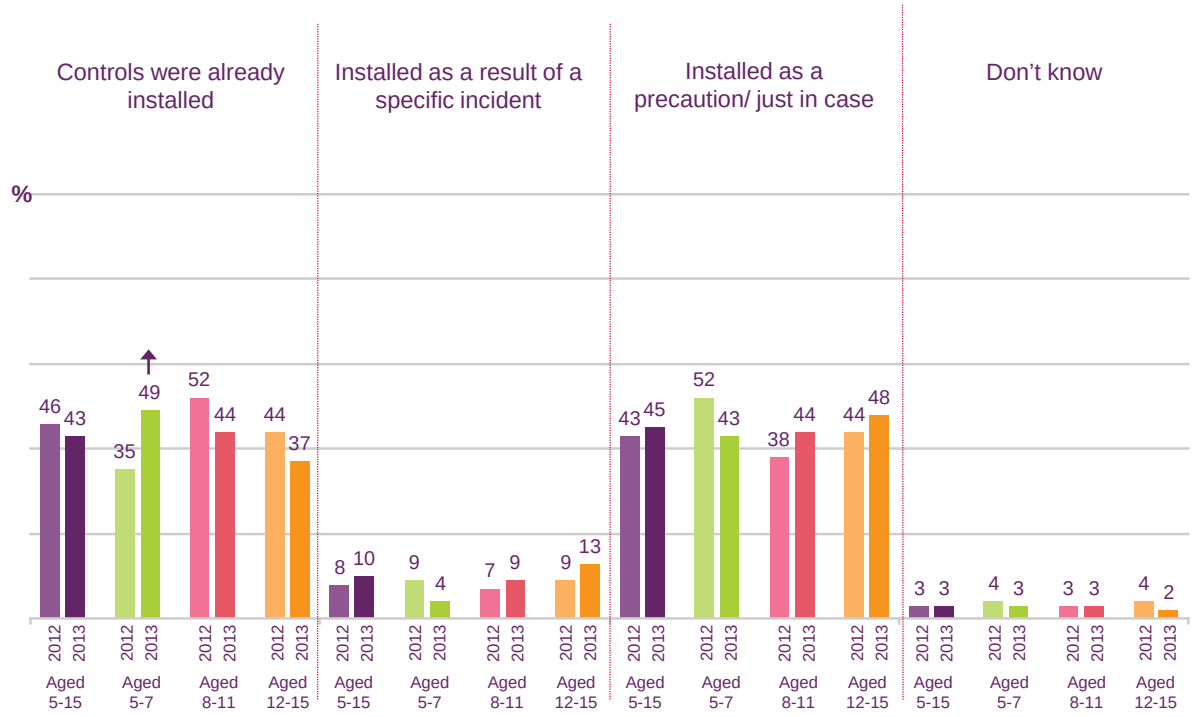
6.48 Around one in 20 parents (6%) say that they have controls installed but they are unsure of the specific type of controls, while one in ten parents (10%) say they are unsure whether they have any parental controls set up/installed.

Reasons for installation of parental controls on the PC/laptop/netbook

6.49 Parents with controls installed on the PC/laptop/netbook that the child uses at home were prompted with a list of possible reasons for putting parental controls in place on the computer, and asked to say which one applied.

6.50 Figure 28 shows that one in ten parents of 5-15s[39] (10%) say that the controls were installed as a result of someone in the household seeing something inappropriate online. Just under half of parents of 5-15s say the controls were pre-installed (43%) or that they were installed as a precautionary measure (45%).

Figure 28: Reasons for installing parental controls on the PC/laptop/netbook that the child uses at home, by age: 2012–2013



QP32 - Please look at the reasons shown on this card. Which one of these describes why the parental controls were put in place? (prompted responses, single coded)
Base: Those parents with any parental controls on the PC, laptop or netbook mostly used by their child to go online at home (650 aged 5-15 in 2012, 594 aged 5-15 in 2013, 186 aged 5-7 in 2012, 164 aged 5-7 in 2013, 248 aged 8-11 in 2012, 246 aged 8-11 in 2013, 216 aged 12-15 in 2012, 184 aged 12-15 in 2013) Significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

6.51 According to the 2012 qualitative study, the main reason given for adopting parental controls was that they came pre-installed on the device or that parents were prompted to install them on purchase or set-up.

6.52 A smaller number claimed to have reacted in response to an incident involving their child or someone they knew encountering inappropriate content. Very few reported that they had implemented parental controls as a precautionary measure. Once parental controls were in place, parents reported that they had tended to forget about them. This could lead to the parental controls falling out of use; for instance where parents had switched them off for their own use and forgotten to turn them back on, where they had not been updated, or where children were using new or different devices to access the internet on which parental controls had not been installed.

[39] Low base sizes prevent analysis among parents of 3-4s with controls installed.

Parental attitudes around the effectiveness of parental controls

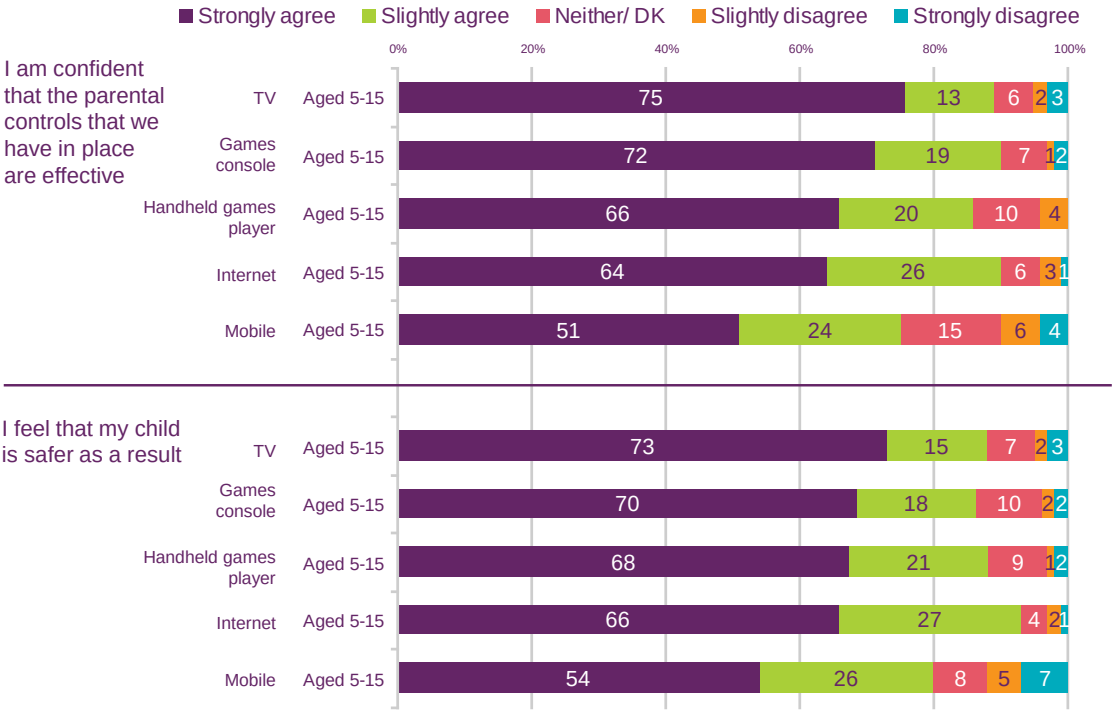
6.53 A majority of parents with controls set on each medium that their child uses feel that these controls are effective and that their child is safe: TV controls score highest and mobile filters lowest.

6.54 Figure 29 summarises the parental attitudes regarding the effectiveness of controls/filters set for internet, mobile phone, handheld games players or fixed games consoles and TV, and whether they felt the child was safer as a result.

6.55 For both statements, around seven in ten parents with controls agree strongly with regard to the controls on their TV services or on the fixed games console, with around two in three in agreement regarding the controls on the handheld games player or their online controls. Around half agree with regard to the mobile phone filters that are in place.

6.56 An interesting comparison with those parents who have installed parental controls is the number of parents who have software installed to protect against junk email/spam or computer viruses. Two in three parents of children aged 5-15 (65%) say they have this software installed (compared to 43% of parents who have parental controls installed).

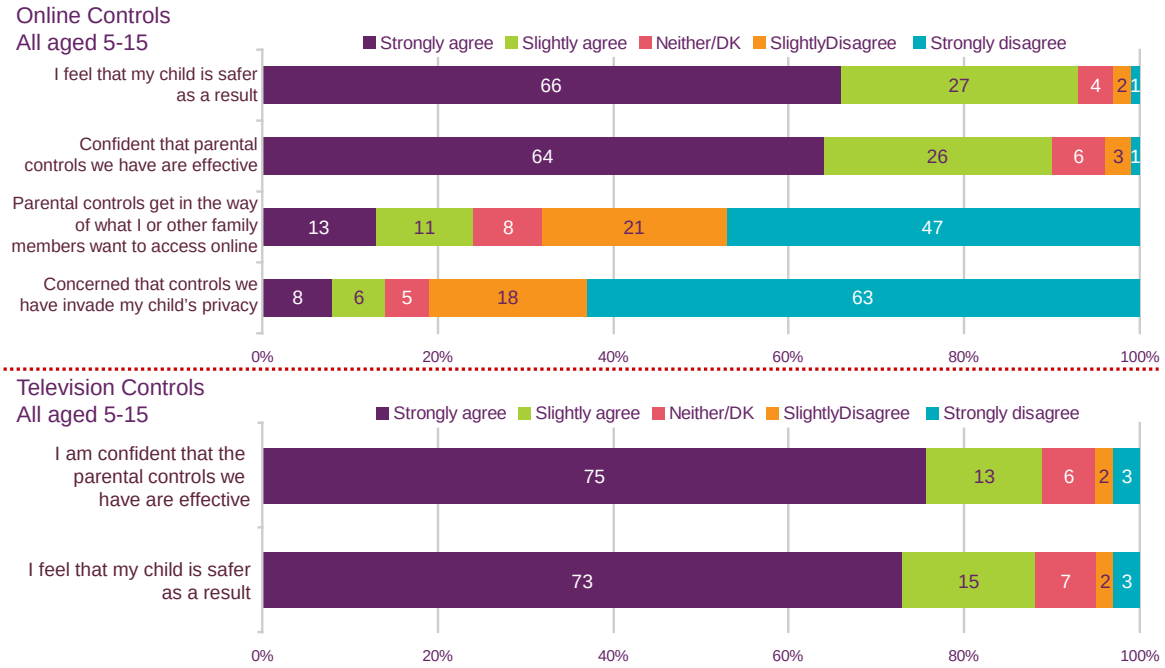
Figure 29: Summary of attitudes towards parental controls among parents of 5-15s, by platform: 2013



QP17A-B/ QP34A-B/ QP71A-B/ QP82A-B/ QP83A-B– Please tell me the extent to which you agree or disagree with these statements in relation to the parental controls that you have in place (prompted responses, single-coded)
Base: Those parents of children with a TV set in the household that the child watches with any parental controls set (744)/ Those parents with any parental controls on the PC, laptop or netbook mostly used by their child to go online at home (594)/ Parents who say their child's mobile phone can be used to go online and controls or filters are set on the phone(202)/ Parents whose child ever plays games at home on a handheld games player with controls set on the handheld games player (150)/
Parents whose child ever plays games at home on a games console connected to a TV with controls set on the games console connected to a TV (207)
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

6.57 Figure 30 below summarises attitudes towards online controls and television controls among parents of 5-15s with each type of control set. This clearly shows that parents of 5-15s with online controls are more likely to believe that their child is safer as a result, and that the online controls are effective, than they are to believe that the controls get in the way or that their child's privacy is compromised.

Figure 30: Summary of attitudes toward parental controls among parents of 5-15s, online and television: 2013



QP17A-B/ QP34A-D– Please tell me the extent to which you agree or disagree with these statements in relation to the parental controls that you have in place (prompted responses, single-coded)
Base: Those parents of children with a TV set in the household that the child watches with any parental controls set (744)/ Those parents with any parental controls on the PC, laptop or netbook mostly used by their child to go online at home (594)
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

6.58 A majority of parents agreed strongly that: "I am confident that the parental controls that we have in place are effective" with parents of 5-7s (72%) and parents of 8-11s (67%) being more likely to agree strongly than parents of 12-15s (55%).

6.59 There are no differences when comparing parents of 5-15s with controls provided by their ISP with parents whose controls were built into the computer's operating system.

6.60 The majority of parents agree strongly that: "I feel that my child is safer as a result of the controls we have" with parents of 5-7s (73%) and parents of 8-11s (70%) being more likely to agree strongly than parents of 12-15s (57%).

6.61 While a majority of parents do not disagree strongly, they do disagree overall with the statement: "The parental controls get in the way of what I or other family members want to access online". Close to seven in ten parents of children aged 5-15 disagree (68%) with this statement while a sizeable minority of parents (25%) agree.

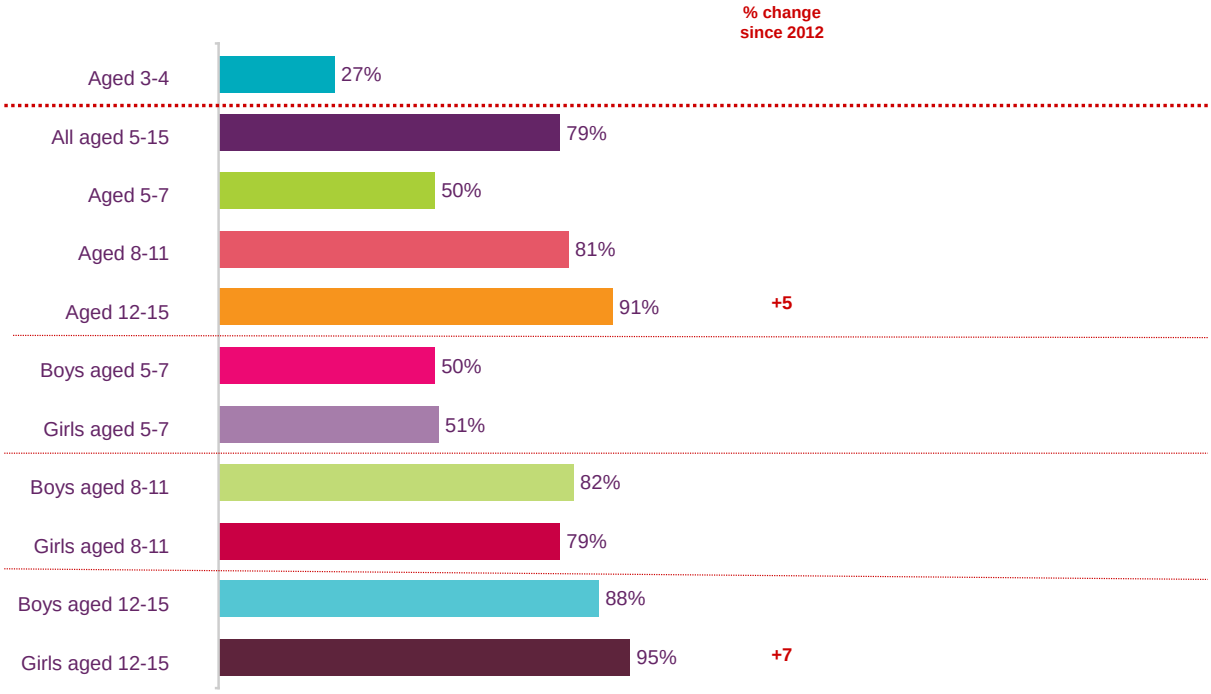
6.62 Parents of 5-15s with controls provided by their ISP are more likely than parents whose online controls were built into the computer's operating system to agree with this statement (29% vs. 19%).

Parental guidance

6.63 Parents who said they talked to their child about staying safe online have been asked how frequently they did this.

6.64 Figure 31 shows that four in five parents of 5-15s who use the internet at home (79%) say that they have ever spoken to their children about staying safe online. This overall incidence is more common among parents of 8-11s (81%) and 12-15s (91%) than among parents of 5-7s (50%) or parents of 3-4s (27%). Parents of girls aged 12-15 are more likely than parents of boys of the same age to have spoken to their child (95% vs. 88%).

Figure 31: Parents who have spoken to their child about staying safe online, by age and gender: 2013

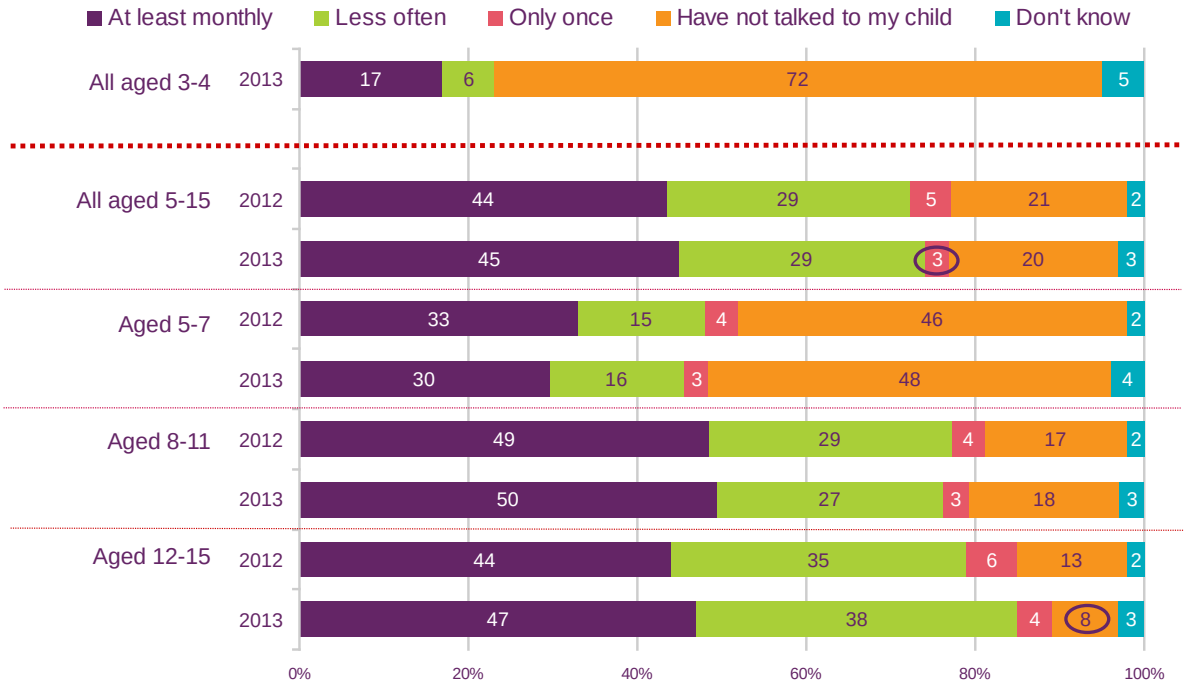


QP54 – Have you talked to your child about staying safe when they are online? (spontaneous responses, single coded)
Base: Parents of children aged 5-15 whose child uses the internet at home (1426 aged 5-15, 381 aged 5-7, 497 aged 8-11, 548 aged 12-15, 187 boys aged 5-7, 194 girls aged 5-7, 195 boys aged 8-11, 187 girls aged 8-11, 219 boys aged 12-15, 217 girls aged 12-15) – significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

6.65 Figure 32 shows that more than two in five parents (45%) of children aged 5-15 who use the internet at home have spoken to their child about staying safe online at least once a month, with this being more likely for parents of 8-11s (50%) and 12-15s (47%) than of 5-7s (30%) or 3-4s (17%). A further three in ten parents (29%) have spoken to their child more than once, but not as frequently as monthly.

6.66 Parents of girls aged 12-15 are more likely to have talked to their child at least monthly, compared to parents of boys aged 12-15 (52% vs. 42%).

Figure 32: Frequency of speaking to their child about staying safe online, by age: 2012–2013



QP54 - Have you talked to your child about staying safe when they are online?/ QP55 Which of these best describes how often you talk to your child about staying safe when they are online?(prompted responses, single coded)
Base: Parents of children aged 5-15 whose child uses the internet at home (219 aged 3-4 in 2013,,424 aged 5-15 in 2012, 1426 aged 5-15 in 2013, 376 aged 5-7 in 2012, 381 aged 5-7 in 2013, 495 aged 8-11 in 2012, 497 aged 8-11 in 2013, 553 aged 12-15 in 2012, 548 aged 12-15 in 2013, Significance testing shows any difference between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

6.67 Parents of 3-15s[40] who have never spoken to their child about staying safe online were asked why this was, and the results are shown in Figure 33 below. Nine in ten parents of 3-4s (90%) and eight in ten parents of 5-7s (80%) say it is because their child is too young for this kind of conversation. Around one in four parents of 3-4s (26%) and 5-7s (22%) say it is because their child is always supervised when online.

Figure 33: Reasons for not having spoken to their child about staying safe online, by age: 2013

	Aged 3-4	Aged 5-7	Aged 5-15
Child too young for this kind of conversation	90%	80%	57%
Child is always supervised when online	26%	22%	23%
Child has learnt about this at school	1%	4%	18%
Have not got round to it	1%	4%	7%
Other parent/ adult has discussed this with child	1%	2%	4%
Don't know enough about this to talk about it with my child	0%	1%	3%

QP56– And can you tell me why that is? (spontaneous responses, multi-coded)
Base: Parents of children aged 5-15 whose child goes online at home who have not talked to their child about staying safe online (154 aged 3-4, 326 aged 5-15, 194 aged 5-7) *** Bases for 8-11 and 12-15 are too low
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

[40] Low base sizes prevent analysis among parents of 8-11s and 12-15.

Section 7

Safety measures on sites regularly visited by children

Key findings

- Parental awareness of the minimum age requirement for Facebook has increased among parents whose child has a profile on this site.
- Nine in ten parents of children aged 5-12 with a profile on Facebook, Bebo or MySpace check what their child is doing when visiting these sites. Almost three quarters of parents of children aged 12-15 check their child's social networking site activity. The incidence of the parent being listed as a social networking friend of their child is very high: accounting 94% of the possible cases where the parent could be listed as a friend.
- Forty-four per cent of parents of 5-15s whose child goes online at home on a PC/laptop or netbook say they have safe search settings on search engine websites.
- One in five parents of 5-15s whose child goes online at home on a PC/laptop or netbook has the safety mode set on YouTube. This figure increases to one in three for parents of children who visit YouTube having the safety mode enabled.
- One in ten parents of 5-15s whose child goes online at home on a PC/laptop or netbook have PIN/passwords set on broadcasters' websites.

Parental awareness of social networking safety measures

7.1 To establish the level of parental awareness of minimum age requirements on social networking sites, we asked parents about the minimum age requirement for using the Facebook website.[41] Figure 34 shows that, of those parents with a child aged 12-15[42] with an active profile on Facebook, 87% are aware that there is a minimum age requirement and 37% of parents of 12-15s are aware that the minimum age for having a profile is 13 years old.

7.2 Among parents of children with an under-age profile on Facebook (children aged 5-12), 21% are unaware that there is a minimum age requirement for using Facebook. Twenty-seven per cent think that their child needs to be older than 13 to have a profile.

7.3 Compared to 2012, parents of 12-15s with an active profile on Facebook are more likely to be aware there is a minimum age requirement (87% vs. 72%) and to be aware that it is 13 years of age (37% vs. 24%).

[41] Given that nearly all children aged 8-15 with an active social networking profile have one on Facebook (96%), this question was asked specifically about Facebook.
[42] Low base sizes prevent analysis among 8-11s, 5-7s or 3-4s.

Figure 34: Awareness of minimum age requirements for having a profile on Facebook: 2012–2013

QP60 Please think about having a Facebook page or profile. As far as you know, is there an age someone needs to have reached in order to have a Facebook profile? IF YES: What age is that? (spontaneous responses, multi coded)
Base: Parents of children aged 5—15 whose child has an active profile on Facebook (437 aged 12-15 in 2012, 366 aged 12-15 in 2013, 215 boys aged 12-15 in 2012, 171 boys aged 12-15 in 2013, 222 girls aged 12-15 in 2012, 195 girls aged 12-15 in 2013, 237 ABC1 in 2012, 199 ABC1 in 2013, 316 C2DE in 2012, 247 C2DE in 2013, 238 parents whose child has an under age profile on Facebook in 2012, 170 parents whose child has an under age profile on Facebook in 2013).
Significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

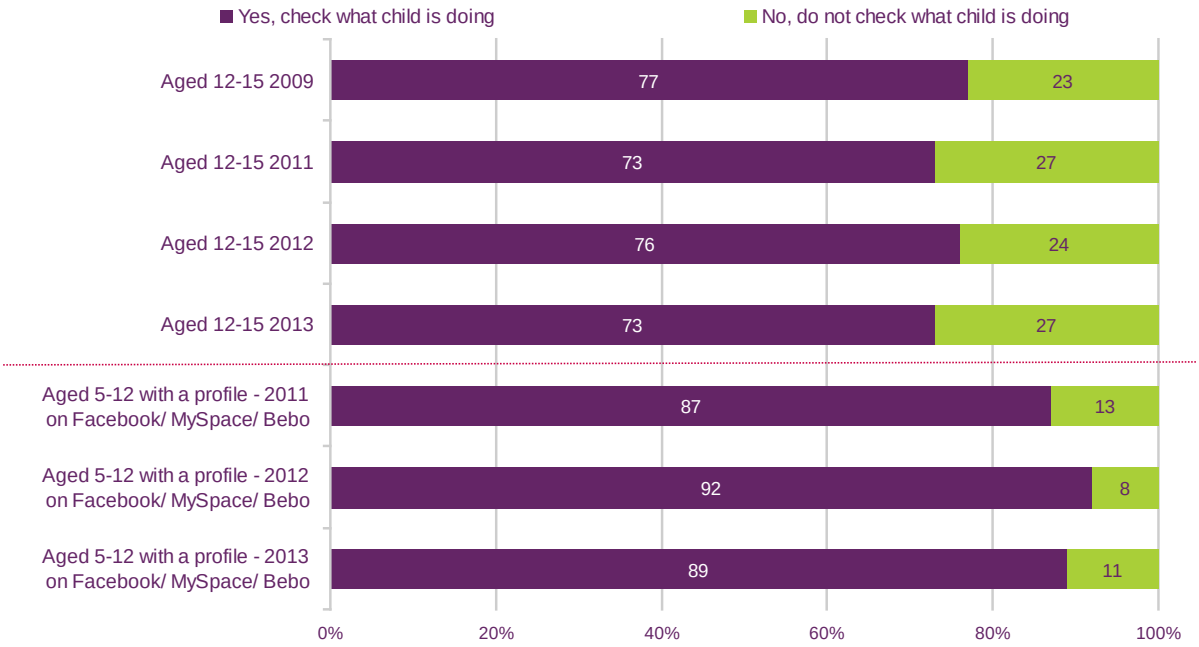
7.4 Parents of 8-15s[43] who are aware that their child has a profile on a social networking website were asked whether they check what their child is doing online when visiting these types of sites.

7.5 As shown in Figure 35, close to three in four parents of children aged 12-15 (73%) check what their child is doing when visiting social networking sites, and this incidence has not changed since 2012. There are no differences in whether checks are made by the child's gender or by the household socio-economic group.

7.6 Nine in ten parents of children aged 5-12 with a profile on Facebook, Bebo or MySpace (89%) also check what their child is doing when visiting these sites; this is also unchanged since 2012.

[43] Low base sizes prevent analysis among 8-11s.

Figure 35: Parental checking of social networking site activity, by age: 2009, 2011–2013



QP48 – Do you tend to check what they are doing online when they are visiting these types of sites? – NB QUESTION WORDING CHANGED AFTER 2009– In 2009 it asked about visits to sites that can be used to 'chat to other users'
Base: Parents of children aged 8-15 with a social networking site profile whose child visits sites that can be used to chat to other users (440 aged 12-15 in 2009, 398 aged 12-15 in 2011, 440 aged 12-15 in 2012, 368 aged 12-15 in 2013, 217 aged 5-12 with a profile on Facebook/ MySpace/ Bebo in 2011, 226 aged 5-12 with a profile on Facebook/ MySpace/ Bebo in 2012, 150 aged 5-12 with a profile on Facebook/ MySpace/ Bebo in 2013). Significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

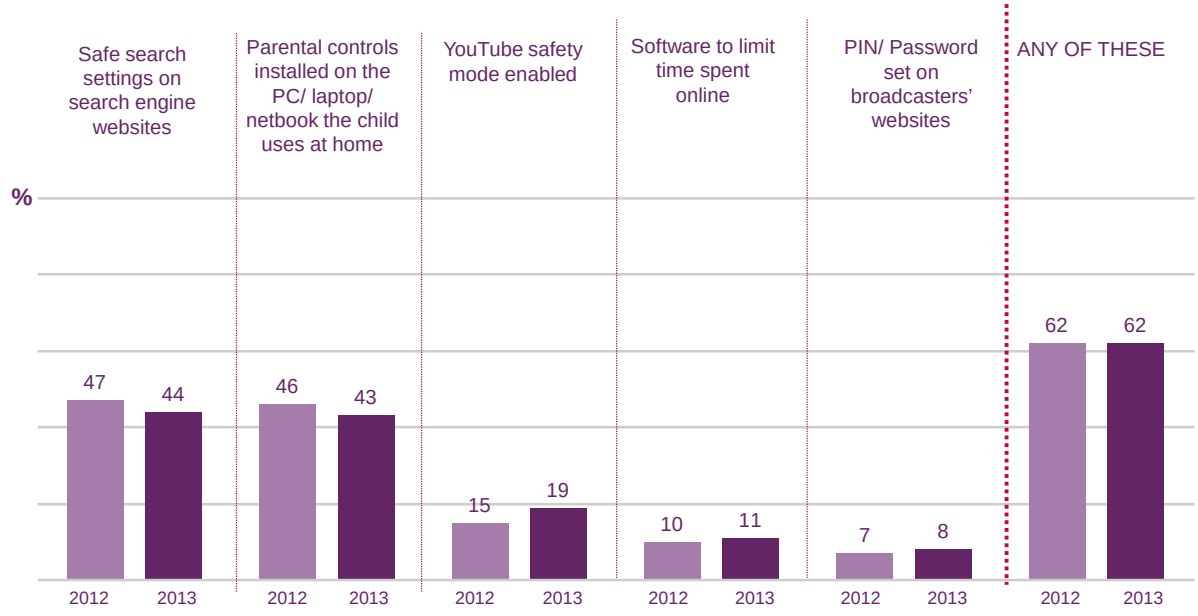
7.7 In 2012, one in four parents of children aged 8-15 (25%) with a social networking site profile, do not have a social networking site profile themselves, with a further 3% having a profile on a site that is not used by their child. Across all of these parents, therefore, seven in ten (71%) have a profile on the same social networking site as their child.

7.8 The incidence of the parent being listed as a friend of their child was very high: accounting for 67% within the 71% where the parent and child use the same social networking site (or 94% of the possible cases where the parent could be listed as a friend). We do not have 2013 findings for this question.

Technical safety measures in place on sites regularly visited by children

7.9 Figure 36 shows that across all of the technical methods of mediation, three in five (62%) parents of children aged 5-15 who go online through a PC/ laptop or netbook have at least one type in place.

Figure 36: Technical mediation in place among parents of 5-15s: 2011–2013



Base: Parents of children aged 5-15 whose child ever uses a PC/ laptop/ netbook to go online at home (1405 in 2012, 1354 in 2013) -Significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

7.10 Figure 37 below provides an age breakdown for the individual technical online controls in place and shows that safe search settings on search engine websites are more likely to be in place for children aged 8-11 (49%) than for 3-4s (37%), 5-7s (40%) or 12-15s (40%).

7.11 Controls on the PC laptop or netbook are more likely among 5-7s (45%) and 8-11s (51%) than among 12-15s (35%).

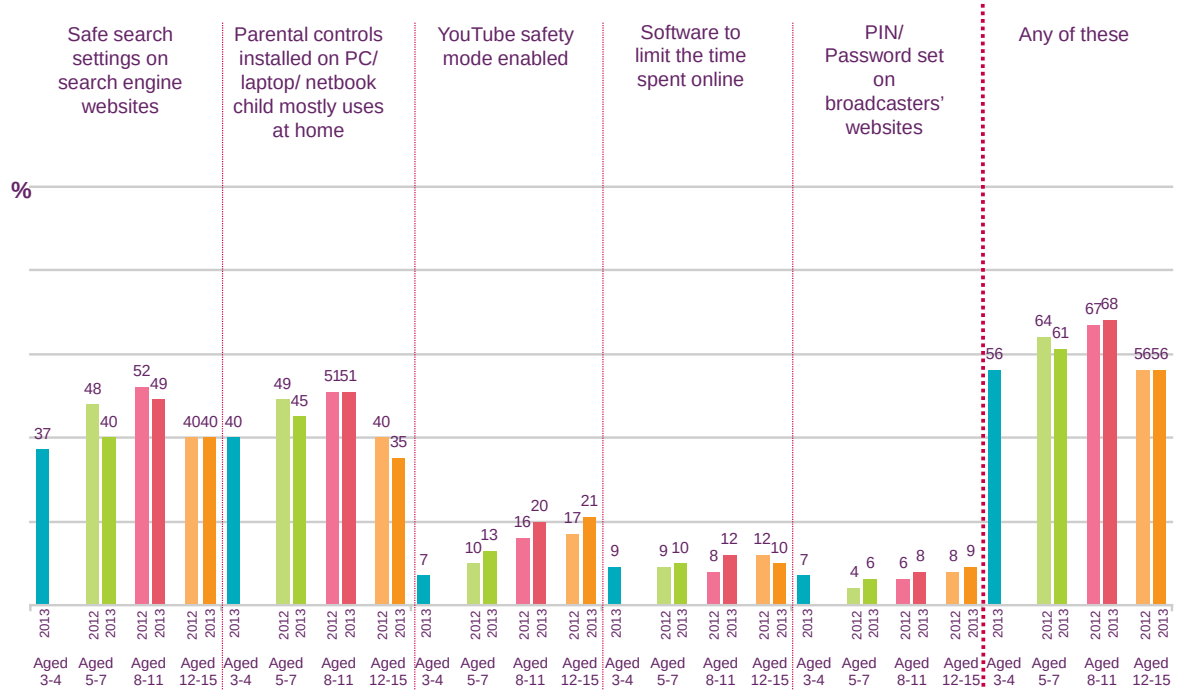
7.12 Parents of both 8-11s (20%) and 12-15s (21%) are more likely than 3-4s (7%) and 5-7s (13%) to have the YouTube safety mode enabled.[44]

7.13 There are no variations by age either in the incidences for software to limit the time spent online, or for PIN/ passwords set on broadcasters' websites.

7.14 At an overall level, households with 8-11s (68%) are more likely than those with 3-4s (56%), 5-7s (61%) or 12-15s (56%) to have at least one of these measures in place.

[44] When parents of children who actually visit YouTube (as opposed to parents of children who go online) were asked about the incidence of enabling YouTube safety mode it increased to one on three.

Figure 37: Technical mediation in place, by age: 2011–2013



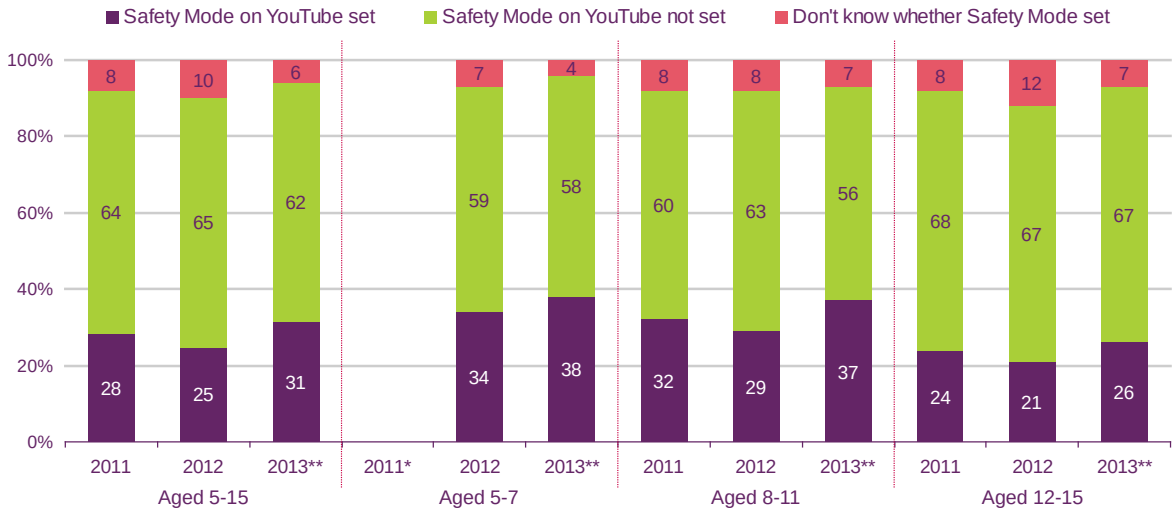
Base: Parents of children aged 5-15 whose child ever uses a PC/ laptop/ netbook to go online at home (1405 aged 5-15 in 2012, 1354 aged 5-15 in 2013, 371 aged 5-7 in 2012, 362 aged 5-7 in 2013, 493 aged 8-11 in 2012, 471 aged 8-11 in 2013, 541 aged 12-15 in 2012, 521 aged 12-15 in 2013). – significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

7.15 In 2013, parents of children aged 5-15 who ever use a PC/laptop or netbook to go online at home were asked whether their child visits the YouTube website through this PC/laptop/netbook.[45] Three in five children who ever go online through a PC/laptop or netbook visit YouTube (61%), with the likelihood increasing with the age of the child, accounting for one in four 3-4s[46] (25%), one in three 5-7s (34%), half of 8-11s (54%) and four in five 12-15s (80%).

7.16 Parents of children who visit this site were asked whether they had enabled YouTube's safety mode to prevent their child viewing some videos. Figure 38 shows that three in ten parents (31%) of a 5-15 year old who visits the YouTube website through a PC/laptop or netbook have the safety mode set. Parents of 5-7s (38%) and 8-11s (37%) are more likely to have the safety mode enabled, compared to parents of 12-15s (26%).

[45] In 2013, parents whose child ever goes online on a PC/laptop/netbook were asked about visiting the YouTube website on the PC/laptop/netbook they use at home, in order to get a more accurate measure of parental controls on the YouTube website. Prior to this, the question was asked of all home internet users (on any type of device) and it did not specify which types of devices they were required to use to visit the YouTube website. As such, results over time are not directly comparable and time series analysis has not been conducted for this question.
[46] Low base sizes of 3-4s who visit the YouTube website prevent any further analysis for this group.

Figure 38: Use of safety mode on the YouTube website, by age: 2011–2013



QP43 - Have you enabled the Safety Mode on YouTube to prevent your child viewing some videos? (spontaneous responses, single coded) **RESULTS BETWEEN 2012 AND 2013 ARE NOT DIRECTLY COMPARABLE DUE TO A CHANGE IN THE WAY IN WHICH THE QUESTION WAS ASKED
Base: IN 2013: Parents whose child visits the YouTube website on a PC/ laptop/ netbook (782 aged 5-15, 124 aged 5-7, 244 aged 8-11, 414 aged 12-15)/Prior to 2013 Parents of children aged 5-15 whose child visits the YouTube website (759 aged 5-15 in 2011, 809 aged 5-15 in 2012, 82 aged 5-7 in 2011, 111 aged 5-7 in 2012, 274 aged 8-11 in 2011, 262 aged 8-11 in 2012, 403 aged 12-15 in 2011, 436 aged 12-15 in 2012) . *Base for 5-7s too low for analysis in 2011. Significance testing shows any difference between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

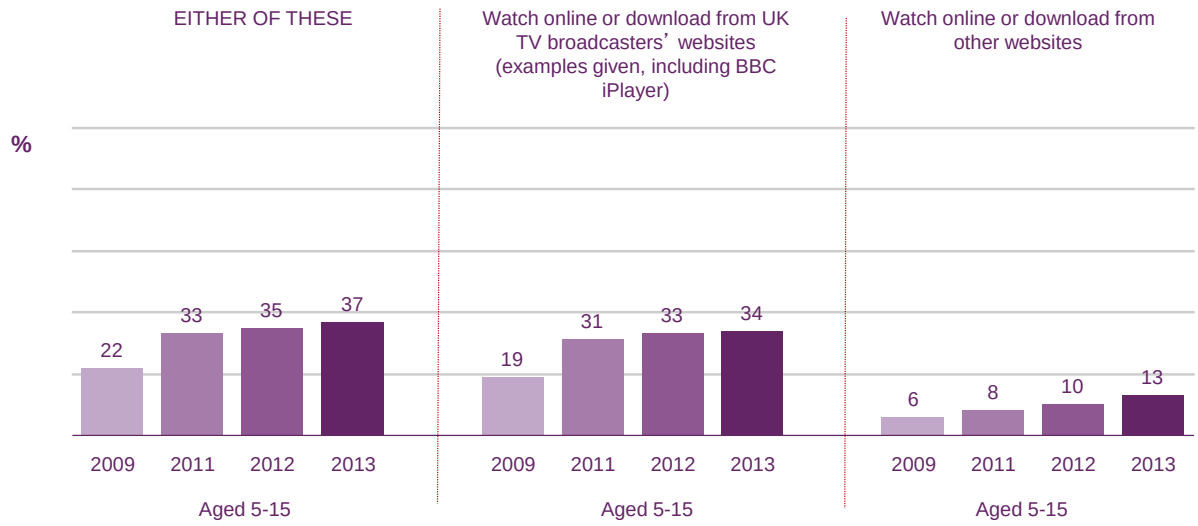
7.17 Parents of children who use the internet at home were asked whether their child ever downloaded or watched TV programmes or films over the internet. The data for children aged 5-15 are shown in Figure 39.

7.18 One in three children aged 5-15 (34%) now watch television content via UK television broadcasters' websites, according to their parents[47], and the incidence increases with age, accounting for one in four (24%) aged 5-7, one in three (32%) aged 8-11 and two in five (42%) aged 12-15. This activity is also undertaken by one in four aged 3-4 (26%), which is comparable to the proportion of 5-7s who have done this (24%).

7.19 Responses for watching content through broadcasters' websites do not vary by the gender of the child, but there are differences by household socio-economic group. Parents of 5-15s who go online in AB households are more likely to say their child downloads content from broadcasters' websites (45% vs.34%) while those in DE households are less likely to say this (27% vs. 34%).

[47]Compared to the responses given by children, parents of 12-15s appear to be less likely to say that their child ever watches TV programmes or films online through broadcasters' websites; 42% of parents vs. 52% of children, although parents of 5-7s appear to be more likely to say they do (24% of parents vs.15% of children). However, the net effect of these differences balance each other out as the overall measure for 5-15s is consistent (34% of parents vs. 35% of children). Children were asked to respond to internet activities shown on a list while parents were asked a direct question about how their child ever watched TV programmes or films.

Figure 39: Watching television programmes and films online, among 5-15s: 2009, 2011–2013



QP50 – Does your child watch TV programmes or films in any of the following ways? (prompted response, multi-coded)
Base: Parents of children aged 5-15 whose child uses the internet at home (1421 aged 5-15 in 2011, 1424 aged 5-15 in 2012, 1426 aged 5-15 in 2013). Significance testing shows any differences between 2012 and 2013.
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

7.20 Parents of children aged 3-15[48] whose child watches/downloads content from UK TV broadcasters' websites were asked whether they were aware that these sites show guidance labels for programmes which may include content unsuitable for young audiences. These parents were also asked whether they had set a PIN or password on any UK broadcasters' websites that their child uses to watch or download TV programmes or films.[49]

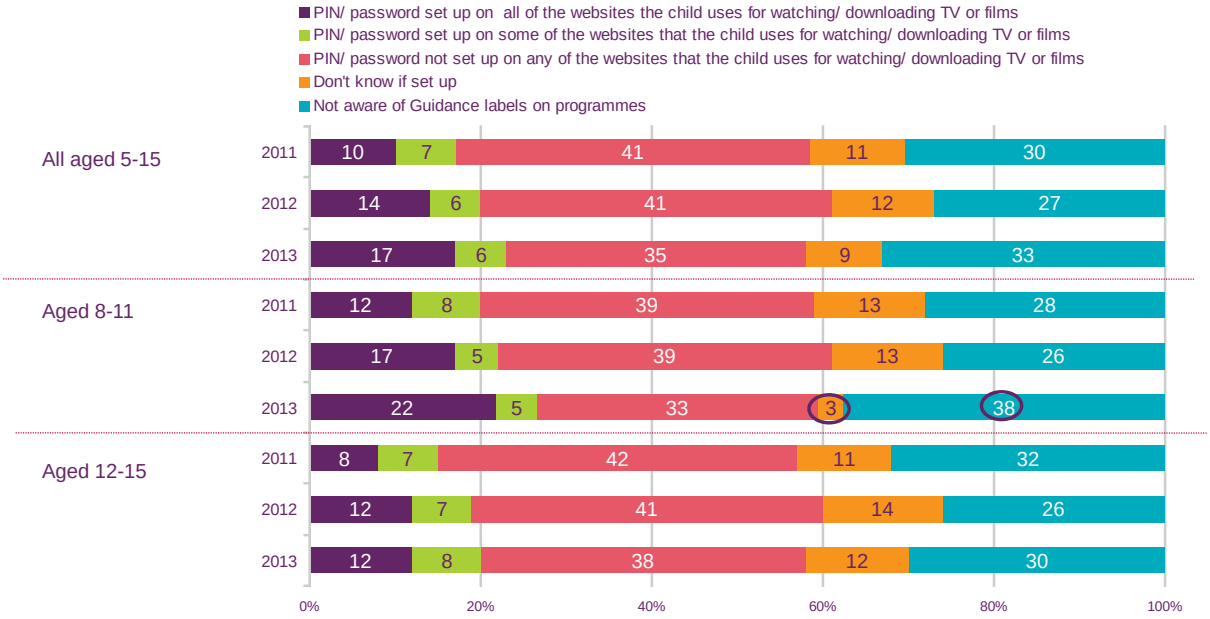
7.21 One third of parents of 5-15s whose child watches/downloads content from UK TV broadcasters' websites (33%) are not aware of the guidance labels for programmes, and around one in four (24%) have set up a PIN/password on all (17%) or some (6%) of the websites their child uses. As such, around one in four of the parents who are aware of the guidance labels have set up a PIN or password to be used before viewing programmes that have a guidance label (24% of the 67% aware of guidance labels).

7.22 Parents of 8-11s are more likely than parents of 12-15s to say that they have set up a PIN/password on all of the websites (22% vs. 12%). There are no differences among children aged 5-15, by gender or by household socio-economic group.

7.23 Around four in ten parents of children aged 5-15 who use the internet at home say they use the 'history' function on the computer to see which websites their child has visited. Use of the history function is much less likely among parents of 3-4s (21%) compared to parents of 5-15s (38%).

[48] Figure 39 does not show data for 3-4s or 5-7s due to low base sizes.
[49] The question wording was changed in 2011 and so we cannot show comparable findings from previous years.

Figure 40: Awareness and use of PIN controls on broadcasters' websites, by age: 2011– 2013



QP51/QP52 – Did you know that UK broadcaster's websites like the BBC iPlayer and ITV Player show Guidance labels for programmes that may include content that is unsuitable for young audiences, (such as violence, sex, drug use or strong language)? / Have you set a PIN or password on the UK websites that your child uses to watch or download TV programmes or films – which needs to be entered before viewing programmes that have a Guidance label? (spontaneous responses, single coded)
Base: Parents of children aged 5-15 whose child watches TV programmes or movies online / download from TV broadcaster's website (388 aged 5-15 in 2011, 415 aged 5-15 in 2012, 453 aged 5-15 in 2013, 119 aged 8-11 in 2011, 139 aged 8-11 in 2012, 145 aged 8-11 in 2013, 200 aged 12-15 in 2011, 220 aged 12-15 in 2012, 221 aged 12-15 in 2013). Base for 5-7s too low for analysis in 2011-2013.). Significance testing shows any differences between 2012 and 2013.
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

7.24 Around four in ten parents of children aged 5-15 who use the internet at home say they use the 'history' function on the computer to see which websites their child has visited. Use of the history function is much less likely among parents of 3-4s (21%) compared to parents of 5-15s (38%).

Section 8

Why parents choose not to apply parental control tools

Key findings

- The most significant reasons for non take-up of parental controls are a combination of parents trusting children to be responsible online and supervising the child. The balance between these factors is strongly influenced by the age of the child.
- A lack of awareness and understanding of parental controls also appears to be a key reason for non-take up. There is a perception, particularly amongst parents with lower levels of confidence about technology, that the process of selecting and installing parental controls was complex and time-consuming.
- The potential value of parental controls does not appear to be front-of-mind on a daily basis for some parents and their focus was more around their children's day-to-day internet use (e.g. children spending too much time online) rather than around the risks which few parents had any direct experience of (e.g. of physical and psychological harm related to exposure).
- In addition, even amongst those who had installed parental controls, many had not given them much further thought and protections may have become outdated as a result of this lack of continuing engagement.
- Overall, parental controls were viewed as a supplement to, rather than replacement for, hands-on parenting. Supervision and other forms of parental mediation were felt still to be needed to manage all of the day-to-day issues their children faced, including risks emanating from children's internet usage.

Reasons for not having parental controls set

Reasons for not having parental controls set on PC/laptop/netbook

8.1 In the 2013 quantitative study, the reasons for not having parental controls installed at home differ considerably by the age of the child.

8.2 Figure 41 below looks at reasons for not having parental controls installed on the PC/laptop/netbook that the child uses at home, among parents of children aged 5-15.

8.3 In 2013, half of this group say it is because they trust their child to be sensible/responsible (49%), with close to four in ten saying there is no need for controls as their child is always supervised (38%).

8.4 The reasons given tend to vary by the age of the child, as shown in figures 42 and 43.[50] The main reason given by nearly two in three parents of 5-7s (62%) is that their

[50] The data in Figure 42 and Figure 43 only show responses given by 5% or more of all parents.

child is always supervised when using the internet; with one in three (35%) saying their child is too young for this to be a problem.

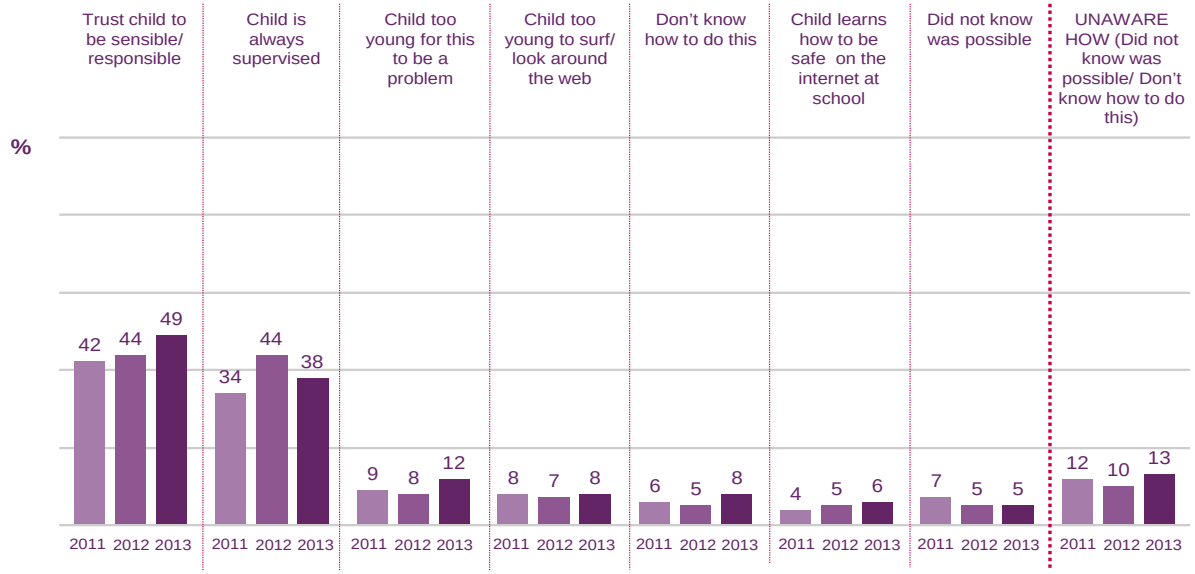
8.5 Around half of parents of 8-11s also say it is because their child is always supervised (53%) or because they trust their child to be sensible/responsible (46%).

8.6 Among parents of 12-15s, two in three (66%) say they trust their child to be responsible, with around two in ten (18%) stating that they do not set internet controls because their child is always supervised. Trusting their child to be sensible/responsible is considerably lower among parents of 5-7s (15%) and 8-11s (46%) compared to 12-15s (66%).

8.7 One in eight parents of 5-15s (13%) say they do not have parental controls installed on the PC/laptop/netbook, either because they don't know how to do this, or they are not aware that it is possible. This is comparable across each of the three age groups of children.

8.8 Parents of boys aged 12-15 are more likely than parents of girls aged 12-15 to say that controls would not work because their child would find a way round these controls (10% vs. 2%).[51]

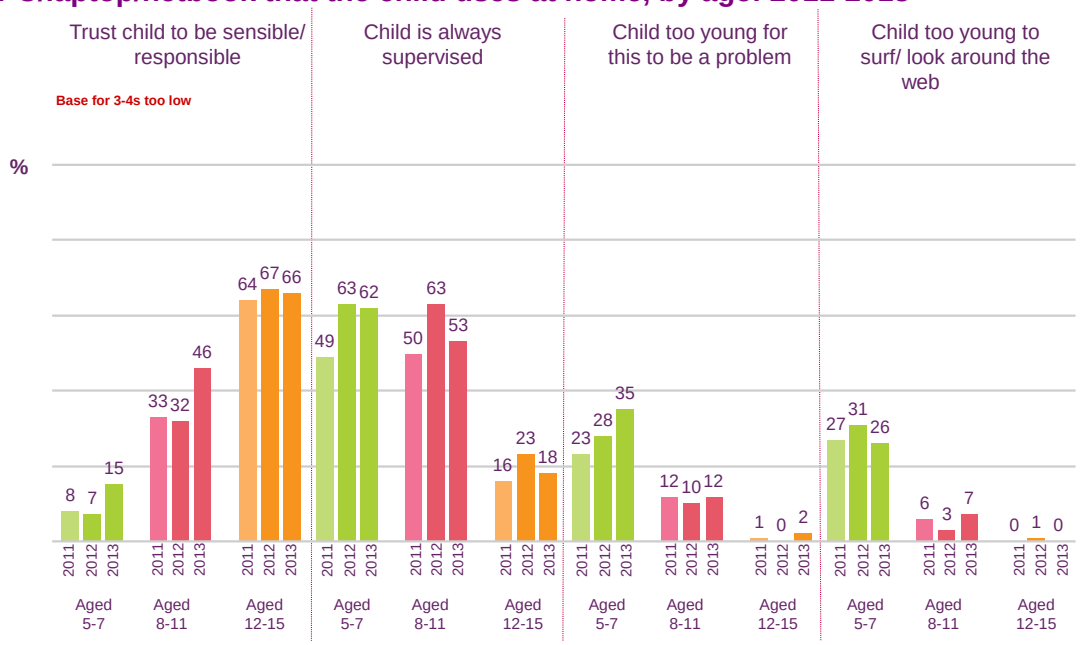
Figure 41: Unprompted reasons for not having parental controls installed on the PC/laptop/netbook that the child (5-15) uses at home: 2011–2013



QP36– And can you tell me why that is? (spontaneous responses, multi-coded) – only responses shown where>5% of all parents have given that answer
Base: IN 2013: Parents that have never had controls set on the PC/ laptop/ netbook that the child mostly uses to go online at home (539 aged 5-15)/ Prior to 2013: Parents of children aged 5-15 without any controls set or software loaded to stop their child viewing certain types of websites (787 aged 5-15 in 2011)/ BASE AMENDED IN 2012 - Parents of children aged 5-15 with no parental controls on the PC, laptop or netbook mostly used by their child to go online at home (607 aged 5-15 in 2012). Significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

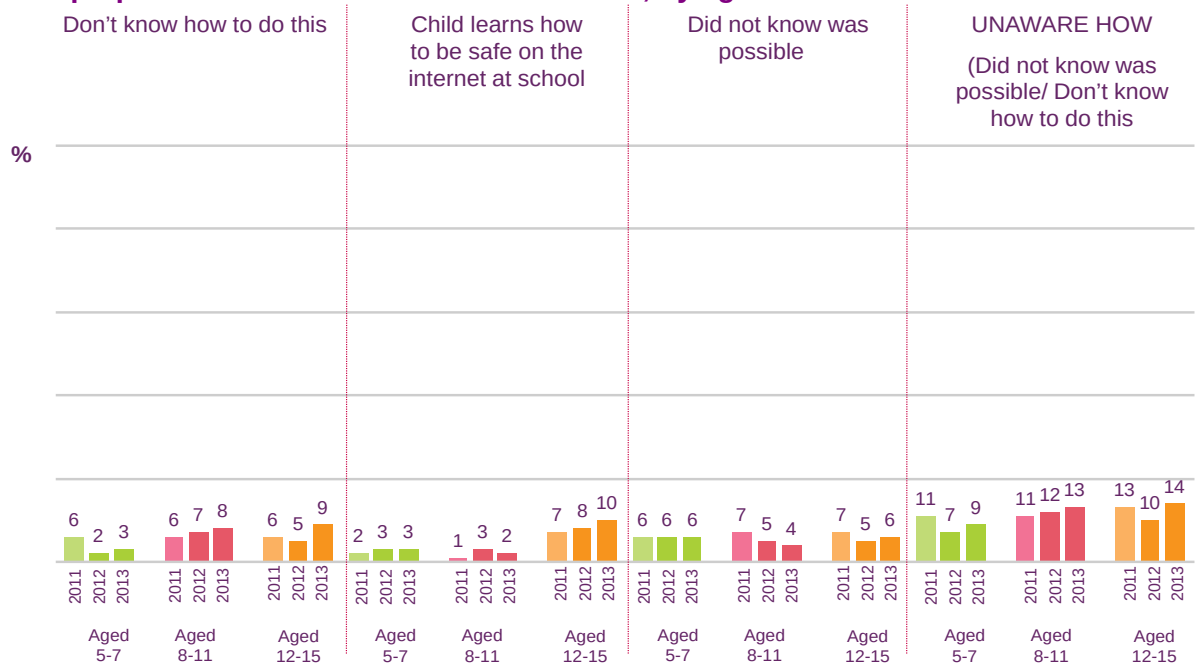
[51] Bases for parents of boys and girls aged 5-7 and 8-11 are too low for analysis.

Figure 42: Unprompted reasons for not having parental controls installed on the PC/laptop/netbook that the child uses at home, by age: 2011-2013[52]



QP36– And can you tell me why that is? (spontaneous responses, multi-coded) – only responses shown where>5% of all parents have given that answer
Base: IN 2013: Parents that have never had controls set on the PC/ laptop/ netbook that the child mostly uses to go online at home (144 aged 5-7, 157 aged 8-11, 238 aged 12-15)/ Prior to 2013: Parents of children aged 5-15 without any controls set or software loaded to stop their child viewing certain types of websites(230 aged 5-7 in 2011, 238 aged 8-11 in 2011,319 aged 12-15 in 2011)/ BASE AMENDED IN 2012 - Parents of children aged 5-15 with no parental controls on the PC, laptop or netbook mostly used by their child to go online at home (155 aged 5-7, 186 aged 8-11, 266 aged 12-15). Significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

Figure 43: Unprompted reasons for not having parental controls installed on the PC/laptop/netbook that the child uses at home, by age: 2011-2013[53]



QP36– And can you tell me why that is? (spontaneous responses, multi-coded) – only responses shown where>5% of all parents have given that answer
Base: IN 2013: Parents that have never had controls set on the PC/ laptop/ netbook that the child mostly uses to go online at home (144 aged 5-7, 157 aged 8-11, 238 aged 12-15)/ Prior to 2013: Parents of children aged 5-15 without any controls set or software loaded to stop their child viewing certain types of websites(230 aged 5-7 in 2011, 238 aged 8-11 in 2011,319 aged 12-15 in 2011)/ BASE AMENDED IN 2012 - Parents of children aged 5-15 with no parental controls on the PC, laptop or netbook mostly used by their child to go online at home (155 aged 5-7, 186 aged 8-11, 266 aged 12-15). Significance testing shows any differences between 2012 and 2013
Source: Ofcom research, fieldwork carried out by Saville Rossiter-Base in April to June 2013

[52] Figure 42 shows responses given by 5% or more of all parents of 5-15s without parental controls set on the PC/laptop/netbook the child uses at home.

Reasons for not having parental controls set for mobiles phones

8.9 In 2013, parents of 12-15s who do not have filters installed on their mobile phones say the main reason is that they trust their child to be responsible (55%). However, a significant minority respond that they are not aware that this is possible (31%) or don't know how to do it (7%). One in 20 parents of 12-15s say it is because their child learns how to use their phone safely at school (6%) or that their child is too old for setting controls (5%).

Reasons for not having parental controls set on games consoles

8.10 Those parents who do not have parental controls set on games consoles were asked to say why. One third of parents say this is because they trust their child to be sensible/responsible (33% for handheld games players and 35% for fixed consoles) and around three in ten say it is because their child is always supervised (28% for handheld games players and 30% for fixed consoles). Around one in ten say it is because the child is too young for this to be a problem (12% vs. 9%).

8.11 Some parents do not use parental controls on the handheld/portable games console, either because they don't know how to do it, or are not aware that it is possible. Being unaware of parental controls in either of these ways accounts for more than one in five parents of 5-15s who do not have parental controls in place (25% for handheld/portable games consoles and 22% for fixed games consoles).

Qualitative reasons for not having parental controls set

8.12 The 2012 qualitative research found that amongst non-users of parental controls there was a widespread lack of engagement with this technology. This was driven by a combination of:

- The perception, particularly amongst parents with lower levels of confidence about technology, that the process of selecting and installing parental controls was complex and time-consuming; and
- The fact that some of the risks of the internet, particularly exposure to inappropriate material, were not top-of-mind for many parents.

8.13 The result was that many of these parents had 'not got around' to installing parental controls.

8.14 In addition, even amongst those who had installed parental controls, many had not given them much further thought and protections may have become outdated as a result of this lack of continuing engagement.

8.15 Also, according to the 2012 qualitative research, the potential value of parental controls did not appear to be front-of-mind on a daily basis for parents. In the absence of a specific trigger many without parental controls admitted 'not getting around' to considering them. Their reported focus was more on the issues and problems that they were regularly incurring with their children's day-to-day internet use (e.g. children spending too much time online) rather than on the risks (e.g. of physical and psychological harm related to exposure) of which few had any direct experience.

[53] Figure 43 shows responses given by 5% or more of all parents of 5-15s without parental controls set on the PC/laptop/netbook the child uses at home.

8.16 Thus, lack of awareness and understanding of parental controls appeared from this research to be a key reason for the non take-up of parental controls compared, for example, to making a conscious decision to reject them.

8.17 In addition, there were some other related factors, including the perception that parental controls were a fairly complex area, and that choosing and installing them would therefore require a considerable investment of time and effort.

8.18 For lapsed users, the most significant factor appeared to be 'forgetting' to re-install if, for example, parental controls stopped working or there was a switch to a new ISP or device within the household. This further highlights the lack of ongoing engagement with parental controls amongst some parents.

8.19 It is also worth mentioning that there were others who regarded themselves as active users of parental controls but who actually were not. Some of these parents were confused about the definition of parental controls. Others had parental controls which, whilst still physically in place, were obsolete because they did not cover the devices currently being used.

8.20 For those who made a proactive decision to install parental controls, it tended to be because the parent felt that the risk to their children of exposure to inappropriate content outweighed the expected effort to install the controls. By contrast, the risk/effort equation was reversed amongst those who did not have them installed. In other words, they tended to feel that the level of risk was relatively low and did not warrant the effort required to research parental controls, work out what the best option is and actually install them.

8.21 However, some admitted that good intentions in this area were not always realised. In particular, rules were not always strictly or consistently enforced, with parents sometimes instead opting for the path of least resistance. With busy lives and relatively few aware of any negative online experiences directly affecting their children, some also admitted that they did not consistently engage with risks on a day-to-day basis. There were also some parents who felt ill-equipped to intervene, both with respect to parental controls specifically and also other forms of mediation, because of their own lack of confidence or competence online.

Annex 1

DCMS letter

Department for Culture Media & Sport

Secretary of State for Culture, Media and Sport
Minister for Women and Equalities
4th Floor
100 Parliament Street
London SW1A 2BQ

T: 020 7211 6000
F: 020 7211 6309
enquiries@culture.gsi.gov.uk

www.gov.uk/dcms

Ed Richards
Chief Executive
Ofcom
Riverside House
2a Southwark Bridge Road
LONDON SE1 9HA

Our Ref: CMS 240583/DC

6 November 2013

Dear Ed

Reporting on internet safety measures

As you know, in the speech the PM gave, on 22 July, on internet safety measures Ofcom was asked to carry out a reporting function. This followed a number of conversations at official level and this letter seeks to formalise those discussions.

To this end, I am requesting that Ofcom provide me with:

I. Report on internet safety measures

- A report, in December 2013, measuring the take-up, awareness of and confidence of parents in relation to parental controls. I would also like this report to: cover the broader strategies parents may adopt to improve children's online safety; the levels of parental awareness and confidence with the safety measures which may be in place on sites regularly visited by children including, but not restricted to, content providers, search engines and social networking sites; and, as far as it is available, any research into why parents may choose not to apply parental control tools.

- A follow up report in December 2014 so that we can track developments on the range of measures outlined above.

II. Report on ISP commitments to offer Parental Controls

- A rReport in Spring 2014 on the measures put in place by BT, Sky, TalkTalk and Virgin Media to meet commitments to implement network level filtering for new customers by the end of 2013. These ISPs have committed to: delivering family-friendly network level filters for all new customers by the end of December 2013. This means a commitment that all new customers, on setting up their new

broadband service with these providers, will receive a prompt inviting them to set up family-friendly filters and, should customers not engage with this process by, for example clicking next, that filters should be applied. Where the filters are in place, these will apply to all devices in the home which connect to that internet connection and, in order to verify that the person setting the filters is aged 18 or over, that a closed-loop email system of notification will be applied.

I recognise that Ofcom's ability to fulfil these requests is contingent on the cooperation by ISPs, and therefore, we will formally ask ISPs for their cooperation, and to provide you with the necessary information. I also understand you are content that you are able to deliver these requests within your current budgets. Lastly, I would ask that, over the longer term, you consider incorporating relevant data captured in these reports into the annual Children and Parents: Media Use and Attitudes Report.

My officials will keep in regular contact as this work progresses. You should not hesitate to raise any questions with them regarding this direction, or any other aspect of this work.

Maria Miller

Rt Hon Maria Miller MP
Secretary of State for Culture, Media and Sport
and Minister for Women and Equalities

Annex 2

Regulatory Context

A2.1 Section 3 of the Communications Act 2003 ("the Act") sets out Ofcom's principal duties in carrying out its functions which 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. In carrying out these duties, Ofcom must have particular regard, amongst other matters, to the vulnerability of children and of others who appear to Ofcom to put them in need of special protection.

A2.2 Ofcom has statutory duties to regulate broadcast television and radio services and "tv-like" Video-on-Demand services[54] both online and on TV platforms like cable. We also have duties in relation to providers of internet access, as part of our regulation of electronic communications markets in the UK. Finally, we have a statutory duty to promote media literacy.

A2.3 The promotion of media literacy is a responsibility placed on Ofcom by Section 11 of the Act[55], and informs three of Ofcom's strategic purposes: to promote opportunities to participate; to protect consumers from harm; and to contribute to and implement public policy as defined by Parliament.

A2.4 Media literacy enables people to have the skills, knowledge and understanding they need to make full use of the opportunities presented both by traditional and by new communications services. Media literacy also helps people to manage content and communications, and protect themselves and their families from the potential risks associated with using these services. The key objectives of Ofcom's research into children and parents' media literacy are:

- to provide a rich picture of the different elements of media literacy across the key platforms: the internet, television, radio, games and mobile phones;
- to identify emerging issues and skills gaps that help to target stakeholders' resources for the promotion of media literacy; and
- to provide data about children's internet habits/opinions and parents' strategies to protect their children online, to inform the work of UKCCIS, which brings together over 200 organisations to help keep children and young people safe online, and other stakeholder organisations such as Get Safe Online.

Ofcom's regulatory duties in respect of Video-on-Demand services

A2.5 As the United Kingdom's independent regulator for the communications sector, Ofcom's principal duty in carrying out our functions (set out in section 3(1) of the Communications Act 2003) is:

a) to further the interests of citizens in relation to communications matters; and

[54] Further details of Ofcom's statutory powers in relation to online Video-on-Demand programming can be found at annex 1e.

[55] Under Section 14 (6a) of the Act we have a duty to make arrangements for the carrying out of research into the matters mentioned in Section 11(1).

b) to further the interests of consumers in relevant markets, where appropriate by promoting competition.

A2.6 In carrying out this duty, Ofcom must have particular regard, amongst other matters, to the vulnerability of children and of others who appear to Ofcom to put them in need of special protection.

A2.7 The Communications Act makes provisions for the regulation of on-demand programme services (ODPS), which are essentially services whose principal purpose is the provision of programmes the form and content of which are comparable to the form and content of programmes normally included in television services, i.e. TV-like Video-on-Demand (VOD) services. These services can be made available on any platform and are subject to a notification scheme if the editorial control of the service is generally based in the UK. Notified ODPS must comply with minimum content standards under the AVMS Directive, which has been implemented in the UK by Part 4A of the Communications Act 2003.

A2.8 Ofcom has formally designated the Authority for Television On Demand (ATVOD) as the co-regulator for editorial content[56], and the ASA as the co-regulator for advertising content. Ofcom remains ultimately responsible for ensuring that providers of on-demand services observe relevant standards.

A2.9 ATVOD has published Rules and Guidance to ensure compliance of all notified ODPS with certain minimum standards.[57] Rule 11 of the ATVOD Rules reflects section 368E(2) of the Communications Act and states that, "if an on-demand programme service contains material which might seriously impair the physical, mental or moral development of persons under the age of eighteen, the material must be made available in a manner which secures that such persons will not normally see or hear it".

A2.10 ATVOD has adopted a precautionary approach to its interpretation of the wording of the Act and includes R18 material (or material equivalent to content classified in that category) as "material that might seriously impair".

A2.11 In the past year Ofcom has imposed financial penalties on three ATVOD notified ODPS for a breach of Rule 11. These sanctions were imposed on the services 'Playboy TV'[58], 'Demand Adult'[59] and 'Strictly Broadband'[60] after these services provided R18 equivalent material without adequate measures in place – a content access control system – to ensure that those under 18 would not normally see or hear it.

A2.12 ATVOD has no rules to regulate abusive content on notified ODPS, i.e. content that is not considered to be hate speech or material likely to incite crime, or does not amount to R18 equivalent material.

[56] http://stakeholders.ofcom.org.uk/binaries/broadcast/tv-ops/designation180310.pdf.
[57] Under the AVMS Directive, which has been implemented in the UK by Part 4A of the Communications Act 2003.
[58] http://stakeholders.ofcom.org.uk/binaries/enforcement/vod-services/Playboy_TV_Sanction.pdf
[59] http://stakeholders.ofcom.org.uk/binaries/enforcement/vod-services/Demand_Adult.pdf
[60] http://stakeholders.ofcom.org.uk/binaries/enforcement/vod-services/Strictly-Broadband.pdf

Other Online Services

A2.13 Ofcom's role in relation to the wider array of internet services is much more limited. As noted above, we regulate audio visual content delivered over the internet through notified ODPS when they are established in the UK; but we have no statutory powers to regulate any other online content.

Annex 3

The legal status of “Mere Conduits” and “Hosts” in the E-Commerce Directive

A3.1 The operation of the internet, and in particular the diversity of services available and the low barriers to entry, depend substantially on the activities of intermediaries like Internet Service Providers (ISPs), search providers and hosts which as described above connect consumers and service providers online, but do not themselves control the services offered or consumed or know what those services comprise.

A3.2 The challenge for policy-makers arises from the fact that intermediaries are not in the business of distinguishing between different services or types of content. They effectively enable the internet to act as a platform for all purposes: for illicit or undesirable ones as well as those which are considered beneficial. The intermediaries policy trade-off is that:

A3.3 Intermediaries play a critical role in the operation of the internet, and hence present an important point of leverage through which the accessibility of unlawful or potentially harmful services might be controlled (especially relevant for overseas content which it may otherwise be difficult to exercise control); but

A3.4 If intermediaries are made responsible for the characteristics of the content and services they transmit or host, they could become liable for any activity online. To manage their own potential liability, they would be strongly incentivised to become internet gatekeepers, determining which services could be accessed and which could not, potentially limiting innovation and freedom of expression, and restricting consumer access to information on the open internet.

A3.5 Under EU legislation – the E-commerce Directive – intermediaries (such as ISPs, hosts and search engines) are protected from having content regulatory obligations imposed upon them. These intermediaries do not know whether the services they carry, index or host are unlawful or potentially harmful, and the Directive exempts them from responsibility for the actions of their users in making content available – even if those users make available unlawful material.

A3.6 The Directive also prevents the imposition of a “general monitoring” obligation on intermediaries, meaning they cannot be required to monitor all the content they are carrying, hosting etc. to determine whether it is legal.

A3.7 The effect of this framework is to create two critical categories of intermediary: *mere conduits* (most importantly ISPs), which only transmit data, and cannot held responsible for unlawful or potentially harmful use of their networks; and *hosts*, including web hosts and social networks, which allow others to offer content online. Hosts cannot be made responsible for identifying illegal content, but can be required to remove content when it is identified as illegal by others – in other words, on an ex post basis.

A3.8 The protections included in the E-commerce Directive, as outlined above, were based an analysis of the trade-offs between

- the economic and cultural benefits which derive from the operation of an open internet;

- the extent to which an open internet delivering these benefits relies on the protection of intermediaries from liability relating to the actions of their subscribers or the characteristics of the online content and services those subscribers choose to access and distribute; and

- the opportunities to secure policy goals by imposing obligations on intermediaries.

Any discussion of intermediaries' roles and responsibilities must take account of both the benefits of liability protection as well as the consumer risks to which an open internet gives rise.