Parental Internet Controls

Consultation Response Form

The closing date is: 6 September 2012
Your comments must reach us by that date.

The Government is keen to take views from information and communication businesses which are members of the UK Council for Child Internet Safety. It is therefore asking for responses to a slightly shorter timeframe than usual so that the process concludes well in advance of the date by which the internet service provider (ISP) Code of Practice is due to be fully implemented in October 2012, but also allowing a reasonable time for responses.

Information provided in response to this consultation, including personal information, may be subject to publication or disclosure in accordance with the access to information regimes, primarily the Freedom of Information Act 2000 and the Data Protection Act 1998.

If you want all, or any part, of your response to be treated as confidential, please explain why you consider it to be confidential.

If a request for disclosure of the information you have provided is received, your explanation about why you consider it to be confidential will be taken into account, but no assurance can be given that confidentiality can be maintained. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

The Department will process your personal data (name and address and any other identifying material) in accordance with the Data Protection Act 1998, and in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties.

Please tick if you want us to keep your response confidential. ☐

Reason for confidentiality:

Name John Carr

Organisation (if applicable) Children's Charities' Coalition on Internet Safety

Address: 10, Great Queen Street London WC2B 5DD

If your enquiry is related to the policy content of the consultation you can contact the Department by telephone on 0370 000 2288 or by email at: ParentalInternetControls.CONSULTATION@education.gsi.gov.uk

If you have a query relating to the consultation process you can contact the CYPFD Team by telephone: 0370 000 2288 or via the Department's 'Contact Us' page.

Section 1: Your details

Please select the category which best describes you as a respondent.

☐ Father	☐ Mother	☐ Grandparent/other family member
☐ Young person under 18	☐ Member of public not described above	☐ Information/communication business
x Voluntary and Community Sector	☐ Academic/Researcher	☐ Other

This submission is made by the following children's organizations: Action for Children, Barnardos, Beatbullying, the British Association of Fostering and Adoption, Children's Society, ECPAT UK, Kidscape, National Children's Bureau, NSPCC, Stop It Now!

If applicable, please confirm the number of children that you have parental responsibility for, and their ages.

All of our member organizations in varying degrees work closely with children and families. The children cover the full age range, from 0 to 17. In several instances staff in our member organizations will be acting in loco parentis.

If you work for information/communication businesses, please specify which sector (e.g. ISP). We will assume you have the authority to represent the views of that business and are not just providing your personal views.

Comments: N/a

Questions in Sections 2 - 4 are directed mainly at parents, and parenting and children's charities. Questions in Section 5 are directed mainly at businesses in the information and communication industries and their trade associations.

Section 2 - What has already been done by the information and communication industries

UKCCIS has been encouraging businesses to develop effective tools to help keep children safe online, including for broadband internet services in the home, mobile phones and other portable internet-enabled devices, public wifi and internet-connected television. The following questions seek your views on how useful these tools are.

1 What existing parental controls on access to the internet and internet-enabled devices do you use to help your children stay safe online? [Please select all that apply]

☐ Blocking particular kinds of content (e.g. sites promoting harmful behaviours, pornography or other age-related material)	☐ Restricting access to a list of chosen safe websites	☐ Using keywords to block (or allow) access
☐ Preventing access to certain internet sites (e.g. social networking sites) at particular times of the day	☐ Preventing access to particular hardware (e.g. cameras or location identification on mobile phones)	☐ Preventing access to particular applications (e.g. web browsers or social networking apps)
x ☐ Other (please specify)		

At different times all or most of our member organizations will use some or all of the tools mentioned.

It should also be noted, however, that many programmes which fall within the general class of “family safety software” do a great deal more than “block, prevent or restrict”, the only three verbs to feature in this question. Some monitor and report what a child does. Others simply provide information about safety issues, often in a timely manner as a particular action is undertaken or is about to be undertaken. Many do all of these things.

Preventing, blocking or restricting access to parts of the internet is what many parents want to do at various points in their children’s journey to maturity, and for good reasons, but it would be a great mistake to think that that is the be all and end all of online child safety.

2 Which of the parental controls you selected in Question 1 do you find the most useful? [Please write in space provided]

This question is too broadly cast for us to be able to respond in the way we think the question is intended. Within our organizations each of the tools will be useful at different times for different purposes with children who have a range of needs.

3 Is there anything that would make it easier for you to use the parental controls already available on the devices and broadband connections you already have? [Please list]

Simplicity is the key

Professor Sonia Livingstone's and other research tells us that parents like the idea of being able to use filters and content management tools to protect their children from harmful or age inappropriate materials, web sites or experiences on the internet. The reason so many parents do not translate this into concrete action is because when it comes to setting up the required software they find the processes and procedures too complicated or too intimidating.

In these matters, therefore, what parents want and children need may be summed up in one word: "simplicity".

The options

Although it is usually possible to install filters and content management tools at any time, typically it is most *likely* this will be done when the internet connection or the internet enabled device in question is turned on or used for the first time. In the context of promoting awareness of online child safety, understandably a great deal of attention is therefore focused on this initial, critical phase.

The Government's consultation paper sets out three options for how, in future, at the point of first use, parents might be presented with an easy to understand and easy to adopt opportunity to use filters and content management tools.

The options are set out at Question 10 (see below). Each is a variant on the theme of "Active Choice". In other words each option would unavoidably require parents to make a decision about whether or not to use a range of filters and tools which are likely to be provided "free" by the vendor of the device or connectivity service. "Free" in this context means the cost would be factored into the price of the device or service and would at no point be presented as being an optional extra that needed to be paid for.

With the provisos stated in our answer we favour option 10 (a). It is the simplest, variously described as "default on" or "opt in".

However, in practice, the differences between the options may be a lot narrower than seems to have been generally supposed in some quarters.

We say this because each of the options are the same to the extent that, by presenting an inescapable screen at the beginning or very early in the sign up process, in effect parents cannot avoid making a decision. Unless and until the decision is made no internet content of any kind is available to anyone.

Please note we do not accept that option 10 (a), or indeed any of the three options on offer in the Government's paper, are inherently any more or any less likely than any other to encourage or discourage either momentary or on-going

parental engagement or parent-child dialogue about online safety.

In matters such as these everything hinges on how the processes are designed and presented and on how they are followed up. There might be any number of "teachable moments" or parent-child talking points built into any and all of the options in the consultation paper or to what follows after the initial Active Choice decision has been made.

Point of purchase or first use and parents

Having acknowledged that the point of purchase or first use presents a golden opportunity to reach out both to parents and children, it is important nobody suggests that if one misses that particular boat all is irretrievably lost and the position can never be recovered.

Yet capturing parents' attention is a key challenge and, while there can be no certainty that it will in fact be a parent that completes the initial processes, at this point in the proceedings it is quite likely at least one parent's attention will be directly engaged, not least because typically they will be paying for something or other or, in order to register a product or commence the service, they will need to present information a child is unlikely to have. If there were any other or additional measures which could be taken to help ensure a parent became involved during these stages they would be greatly welcomed.

Accessible language is hugely important. The intelligent use of pop ups transmitted during the various stages of sign up or on registration will also help bring online child safety to the fore and increase understanding of them.

Intuitive icons presented in a timely way can help enormously, especially if linked to a larger plan to send well designed, user friendly reminders or refreshers to both parents and children at appropriate intervals.

The importance of paper

Many parents or others who are perhaps less confident internet users might find information that is presented to them on paper or another tangible medium easier to assimilate than information that is presented solely online, at least initially. This does not mean companies should choose between the real world and the virtual one. Both have a part to play.

Full information about the choices to be made

During or before the sign up processes companies should provide information about key online safety concepts, and in particular they should explain their own safety arrangements. This should include a description of how their Active Choice system works, what it covers and how to make any changes to it if for

any reason a parent changes their mind after the initial installation processes have been completed.

Such information might be placed inside the box or other packaging that a product comes in or otherwise it should be routinely provided at the point of sale. Alternatively if a product is bought online or a new internet connectivity service is taken up online the information should be sent through the post to an appropriate address

The mobile phone companies' approach

Since 2004 the UK's mobile phone networks have had in place an extremely simple and effective default on or opt in system.

Mobile phones can provide access to content in a number of different ways. Although each is important, in the context of the discussion raised by the consultation paper the immediate focus is on two of them.

The first relates to material which, in one way or another, the mobile phone companies themselves publish or co-publish. The second concerns material which is potentially accessible to anyone because it is on the internet.

In relation to content which the mobile phone companies publish or co-publish the mobile networks decided that everything of that sort had to be labelled as being either "adult" or "universal". If it is adult it goes behind what is often referred to as the "adult bar"

To assist the classification of content which they publish or co-publish the mobile companies created an independent organization, the Independent Mobile Classification Body (IMCB).

The IMCB developed a classification framework which publishers use. Inter alia the IMCB also adjudicates on any disputes which might arise in relation to the operation of the policy. The criteria used for making classification decisions are publicly stated.

For material available via the internet typically the mobile companies use commercially available filtering products. However, they ensure that when they are deployed on their networks these products' filtering criteria are aligned with those of the IMCB. In this way adult content on the internet also goes behind the same adult bar.

The material covered by the adult bar includes pornography but is not restricted to it e.g. it includes sites that promote alcohol, tobacco or self-harm.

The mobile phone companies found an ingenious way of making the policy

work. With some variations, in effect they decided to assume every SIM card user is a child until proven otherwise.

Thus, if a user wants to have access to material behind the adult bar all they have to do is ask their network to unlock it and be able to show their network they are over 18. This can normally be done in sub-two seconds, in line, in real time and inexpensively.

Since 2007 similar systems have also been working very well for the whole of the online gambling industry, where 18 is again the minimum age. Many other companies selling products or services which are meant for persons aged 18 or more make use of already available robust age verification technology that is highly scalable.

One of the reasons the gambling industry, the mobile phone networks and other companies can do what they do by way of age verification is because 95%+ of all adults in the UK are on one or more databases which, with permission, they can access. For anyone who is not on such a database, or who does not want to be authenticated in this way, alternative methods are available e.g. they can take proof of their age into one of the companies' shops, send it through the post. If only partial proof is available some systems allow users to answer a range of questions administered over the telephone. These options introduce a short delay in completing the processes but it means sooner rather than later 100% of the adult population can be included.

Returning to the mobile phone networks, as we have noted, the above arrangements have been operational since 2004 and with no obvious adverse impact on the mobile companies' corporate profitability, user satisfaction with the service, free speech or artistic expression.

Our starting point, therefore, is that as far and as closely as possible, systems should be introduced into the fixed line and WiFi environments which mirror the arrangements currently made by the mobile phone companies.

WiFi and the importance of "seamless safety"

We want to emphasise the importance of bringing WiFi within the ambit of this debate. We believe this proposition is no longer regarded as being controversial by most of the large WiFi providers but it bears repeating for emphasis and for the sake of completeness.

We are rapidly moving towards a highly converged digital environment where, with the spread of publicly accessible WiFi and soon other new wireless technologies, internet access will be ubiquitous. It may not be too far-fetched to say that in parts of our major cities we are already there.

Fixed line access providers normally provide a WiFi router as part of their standard package to families across Britain. Thus, for these purposes fixed line providers must be included in the wider discussion about WiFi.

Our view is it should not matter *which* device your child uses to connect to the internet or *how* or *where* they make the connection to the internet. Parents are entitled to a reasonable expectation that something as fundamental as online child safety has been properly taken into account by each and every access provider and device manufacturer. “Seamless safety” should be the watchword.

It is not unusual for homes to have upwards of a dozen different easily portable internet enabled pieces of equipment being used by various family members e.g. games consoles, iPads, iPhones, iPods, laptops, tablets of various kinds, and smartphones. In addition there may be a more conventional computer in a fixed place and increasingly internet enabled TVs will be a feature of the modern home.

Many of the devices, including most of the portable ones, will be able to connect to the internet via WiFi, often out of the line of sight of the parents. If a child’s friend brings a WiFi enabled device with her in her pocket or school bag whilst on a visit, a parent would have no practical way of knowing that an extra gadget was now on the premises. Indeed it is entirely possible that a family’s WiFi signal will be strong enough to reach out into the street, the garden, the next door neighbours’ flats or houses potentially allowing other (unknown) children and casual strangers who just happen to be walking by or parked outside to access the internet using their facilities.

Internet enabled devices are produced or supplied by a large and eclectic mix of companies of various sizes. Moreover, leaving aside considerations about temporary visitors, there might be a fairly constant ebb and flow of them coming in and going out of a family home as new ones are acquired or old ones are lost, broken and replaced. In such circumstances, whilst locking down the WiFi by keeping the router’s password secret is one option it is not always satisfactory or practical.

Learning to keep passwords secret is an important part of any internet security strategy but we know from experience this will not work if the password is likely to be in constant demand from several different members of the household perhaps at all kinds of random times. Many routers come with the password printed on a label stuck on the side or underneath, put there by manufacturers, and if it isn’t lots of households affix a post-it note there or on the fridge door.

Safety by default

In relation to the wide range of internet enabled devices that are available parents should not have to learn a whole new language of safety, or have to understand possibly several different companies' configuration processes and approaches to online safety every time a new internet enabled device comes through the door.

This means all WiFi and fixed line providers must build in a minimum standard of child safety and turn it on by default.

If every hardware and device provider were to preinstall and preconfigure safety software to a given minimum standard and turn it on by default it would achieve a similar result. However, it is likely to be much more difficult to get to a point where that will happen with manufacturers as compared to WiFi and fixed line connectivity providers. The reason is fairly obvious: the fixed line and WiFi access providers, almost by definition, are going to be UK based and they are smaller in number.

Reliable figures for which companies have what share of the public WiFi market are not yet available. However, at the moment in the fixed line space four companies – Sky, BT, Virgin and Talk Talk - between them have around 92% of the domestic broadband market. If two more companies are added – O2 and Everything Everywhere - the proportion starts to hover around 99%. It is widely thought that these companies are likely to achieve a similar level of dominance of the public WiFi market as it matures

Either way, it is really important that the objective of including WiFi in this policy is achieved. If it is not, increasingly it will make the mobile phone companies' current substantial expenditure on maintaining their adult bar look pointless because it is so easy for any smartphone user, or the user of any other WiFi enabled device that might utilise their networks, to avoid their controls by the simple expedient of signing on to the nearest available WiFi hotspot.

It would indeed be perverse if, by failing to act in this respect, UKCCIS in effect reduced the overall level of online child safety by opening the way for the mobile companies to abandon their current practices. What would be the positive reason for the mobile phone companies to carry on doing what they are doing when all about them everyone else refuses to do anything similar?

If "seamless safety" was in place, covering all fixed line and WiFi access, it would not necessarily eliminate the need for or desirability of hardware and device manufacturers pre-loading safety features, neither would it automatically eliminate the need for them to continue to provide information to their customers about online safety. All companies at all parts of the value chain will continue to have a responsibility to ensure and promote the safety of their

users, particularly younger users. However, in a world where everyone knew that a basic level of online child safety was being built in to every internet access provider's offering, the nature of manufacturers', retailers' and individual service providers' responsibilities would undoubtedly be different.

Our key or overarching point is that parents should not have to jump through hoops to make going on the internet safer or as safe as it can be for their children or their children's visiting friends. Today it is very common for anti-spam and anti-phishing software or firewalls to be turned on by default to protect individuals and the network. We think the same principle should now be extended to online child safety.

No need to declare what adult material you are interested in

As previously noted, under the system used by the mobile phone companies, to gain access to any adult content it is necessary only to ask and be able to prove that the account holder is 18 or above. It is *not necessary for anyone to declare which type of adult content they are interested in or what they want to access.* It is an "all or nothing" approach. This seems to us to be reasonable as it avoids any individual having to declare to anyone that they have a particular interest in, say, pornography, or alcohol, gambling or what have you.

This approach also avoids the potentially ludicrous result, implicit in some of the suggested solutions described in the consultation paper, which would give parents an option, say, to block their child's access to sites promoting alcohol, drugs or knives, but allowing the same child to have access to sites promoting or providing pornography, self-harm, suicide or terrorism.

Age verification

The absence of any reference in the consultation document to age verification is surprising given that it was favoured by Claire Perry, Reg Bailey and Tanya Byron. In our view it is an essential component of any Active Choice solution worthy of the name. The Government should endorse it in whatever option they finally favour.

We acknowledge that in those households that want to allow one or more members to have access to adult content the approach we are suggesting will require individual accounts to be created. The holders of these accounts will need to be age verified.

Our view is that, as with the rules about entry to cinemas, pubs, buying cigarettes and so on, as long as the age verification process is not unduly onerous or time consuming people are likely to accept it because they understand and sympathise with the underlying policy objective, in this case the protection of children. At worst it will be seen as a minor irritation.

The systems adopted by the mobile phone companies and the online gambling industry only require an individual to be age verified once. From that point on the user has an authenticated age verified log in. In fact systems could be created which would allow individuals to get themselves age verified once and for that to be accepted by every or many service providers and device manufacturers. It might also pay dividends in terms of data minimization policies i.e. it would enable a person to prove they were over 18 without having to surrender any other information about themselves.

Of course households are not the same as mobile phones. A mobile phone is a personal device. A telephone number is the equivalent of an individual account and therefore is ready “out of the box” to configure various settings around it. By contrast a home is a communal environment where there may be people with a wide range of ages living under the same roof and where one or more devices might be used regularly by several of them.

For such shared devices some operating systems already allow users to configure individual accounts on the same machine and for each user to be granted different access rights on the basis of their age. This is the case with Microsoft’s X Box for example. Filtering and content management tools provided by specialist companies such as Symantec can also do the same.

Thus, in a sense, what we are proposing “simply” requires a similar approach to be migrated to the systems being used by fixed line and WiFi access providers. This is not a major conceptual leap.

Big step

Although we do not accept that what we are suggesting in this submission is a major conceptual leap we appreciate that introducing age verification for adult content on the wider internet, taking it beyond mobile phones, online gambling and the like is a major and radical step. It would be a world first.

The UK has been first in the world before in the context of online child safety. It is no stranger to taking major and radical steps in this space. Moreover we contend that this approach fits with the direction of travel in relation to other developments on the internet, particularly at EU level, where there is an increasing emphasis on authenticating users and their key attributes, of which age is undoubtedly one.

We are ***not*** arguing that every internet user should be authenticated by reference to their age or any other attribute in respect of every internet transaction they might undertake. Our comments are restricted solely to those parts of the internet which provide or supply content or services which either by law or policy are or ought to be restricted to adults.

A note about sub-18s

As we have already noted it is extremely easy and inexpensive to age verify persons aged 18 or above. What is much harder to do, though not impossible, is to verify ages below 18. However a sub-18 option is not being discussed in this consultation, it is not on the table at the moment nor are we arguing for it here.

That said if companies wished to develop more granular approaches for sub-18s we would be delighted. However, this should not be used as a reason for delaying action on materials which, by any reckoning, ought to be restricted to persons aged 18 or more.

Technical

Technically, there is no question that something akin to what the mobile companies do could be replicated in the fixed line and WiFi environments although we are not in a position to provide an estimate of the costs, timescales or the scale of the engineering that this would entail. Each time we have raised the matter it has been dismissed out of hand with references to it being disproportionately expensive or difficult. We do not think the question was ever given adequate scrutiny or consideration by a disinterested expert third party.

However, the above notwithstanding we believe that, in a home environment, if all of the necessary software and controls were put on the router, rather than the network, it would likely be a great deal cheaper, quicker and easier to implement and subsequently to manage the sorts of changes which we advocate. Routers which do this and which work with individual, age-based log ins are already available on the market.

Content, services and apps

Many of the world's largest internet companies are not involved in providing connectivity services in any significant way. Facebook and Google are the two most obvious examples. It is understood that how companies like these behave, how they treat issues such as privacy, their rules about permissible conduct, how they respond to abuse reports from children, how they moderate or mediate user generated content, their online advertising practices and so on, are hugely significant in terms of the overall online child safety debate. In that context how the new generation of apps are age rated and sold is becoming increasingly important. No settled or reliable independent system in which consumers can repose their confidence has yet emerged.

However, it would complicate the discussion around Active Choice beyond reason and manageability if we were to conflate questions which are specific

and exclusive to how a user connects to the internet with the separate considerations which apply to content, services and app providers.

It is very much the case that every company in the internet value chain has a responsibility to promote as widely as possible a safer internet for children but that does not mean each one must discharge it in an identical way. Policies need to be tied to specific functionalities. This consultation and our response to it is very much focused on Active Choice which is principally about what can be expected of access providers.

Companies not involved

The consultation paper is silent about how the Active Choice initiative is to be carried forward to those companies that do not participate in UKCCIS. How are the "uninvolved" to be brought within the purview of the policy? It is appreciated that while several larger players are actively engaged with UKCCIS, not all of them are. It would be highly undesirable potentially to award a competitive advantage to non-participants over participants by allowing non-participants to avoid investing in or making recommended alterations to their systems just by staying away or not signing up.

4 Did you know that the four main internet service providers, BT, TalkTalk, Virgin Media and Sky, have signed up to a code of practice which says that they will:

- Provide parental controls free of charge
- Provide all new customers with an enforced choice of whether or not to use parental controls
- Improve the communication of information to parents explaining the benefits of parental controls

  Align the information they provide to parents so it is all consistent (i.e. information from BT will be consistent with information from TalkTalk, and so on)

x Yes	☐ No	☐ Not Sure

Comments:

5 Is there anything you think should be added to the code of practice, saying what internet service providers should have to do, or anything that should be taken away? [Please write in space provided]

We can see that there are two aspects to this. How you handle new customers and how you handle existing ones. Any outcome must as far as possible seek to provide existing customers with choices that are the same as or similar to the choices offered to new customers. Existing customers should be required to make a choice. At the conclusion of the current process if Option 10 (a) is adopted as the option most favoured for new users a way of presenting it to existing customers will need to be devised.

The timescale within which ISPs intend to deliver on their promises, for new and existing customers, should also be clear.

For the reasons given earlier, WiFi coverage has to be part of the final package of measures although we can see that WiFi may be a little out of step in terms of the timing of its delivery.

Section 3 - The role of parents

Parents are used to protecting their children from harm when they are very young, and, as they grow up, teaching them how to be safe as they start to explore the world for themselves. The same principles apply to online safety. The internet is a resource for entertainment and information: but some of this material is suitable only for adults and sometimes the deliberate action of others, such as online bullying (‘cyberbullying'), can be harmful.

The following questions seek your views on the role of parents in child internet safety.

6 When it comes to keeping children safe online

☐ Parents have the main responsibility	☐ Businesses have the main responsibility	x Parents and businesses have a shared responsibility

7 Which of the following types of internet content and online behaviour do you know for sure that your children have been exposed to? [Tick all that apply]

☐ Alcohol and drugs	☐ Anorexia/bulimia	☐ Bullying
☐ Gambling	☐ Grooming	☐ Personal abuse of social networking sites
☐ Political or religious radicalisation	☐ Pornography	☐ Self-harm
☐ Sexual messages	☐ Suicide	☐ Violence
☐ Other [please specify]		

The principle has to be that any categories that are used by filters are based on what is harmful to children.

There are no technical challenges associated with collecting data about sites or online content which are harmful to children. All of the filtering companies already have the data and have been collecting it for many years. More or less any configuration or combination of sites could be assembled without any difficulty.

However, the list given here at Question 7 goes way beyond any that we have previously seen and certainly it is much larger than the list used by the mobile phone companies. The phone companies' categories are smaller in number but manage to capture the same range of things under fewer headings. This helps retain the simplicity of the system. Why was what the mobile phone companies do not presented as an option?

8 Which types of internet content and online behaviour do you think most worries your children? [Tick all that apply]

☐ Alcohol and drugs	☐ Anorexia/bulimia	☐ Bullying
☐ Gambling	☐ Grooming	☐ Personal abuse of social networking sites
☐ Political or religious radicalisation	☐ Pornography	☐ Self-harm
☐ Sexual messages	☐ Suicide	☐ Violence
☐ Other [please specify]		

All of the above. It would be difficult to rank these in any sort of order of priority. They are all important and could arise at some point or other in a child's or young person's life according to their individual needs.

9 Which of these issues listed in Questions 7 and 8, do you think you need most help protecting your children from online? [Please write in space provided]

All of the above if the need is there.

The following questions seek your views on the ways of helping parents keep children safe.

10 a) A system in which some internet content (for example, pornography) is **automatically blocked for you** by your internet service provider or by the smartphone or other device you use to access the internet and you can later ask them to remove the filters if you want to access the blocked websites.

x Yes	☐ No	☐ Not Sure

As previously indicated in answer to question 3, this is the option which we support, linked to an age verification process to determine access rights to adult materials. However, we have two important caveats.

Under no circumstances should sites such as Childline, the Samaritans or others which are relevant to children's health, welfare, education or their rights be included in any default on, opt in or other filtering or blocking system which is aimed at protecting children and young people. Moreover, to the extent that parents do deploy filters, content management or monitoring tools it is essential they are used with proper respect for the evolving capacities of the child and a child's right to privacy, free speech, free expression and freedom of association. Equally they should be used in ways which do not corrode trust within a family.

Secondly whatever option is chosen, including option a, as previously mentioned it is essential that parents and children are fully informed about the types of sites and materials which would be affected by any blocking or filtering mechanisms being offered. An explanation should also be provided in relation to what one needs to do if one later changes one's mind about any of the choices made.

Transparency is vital throughout

Whatever option is finally endorsed and implemented, other questions potentially will arise as to its operation e.g. even though the classes of material being filtered may be clearly stated - "pornography", "self-harm" and so on - there may well be legitimate concerns about how well the filters actually work.

Are the filters doing the job they are meant to do? There will always be a degree of under-blocking and over-blocking but is this taking place within acceptable tolerance levels? Can we be confident the filters are not blocking access to classes or types of sites, or individual sites, which ought not to be blocked? Is there a satisfactory mechanism for quickly resolving any disputes about a site being incorrectly blocked or classified?

If different companies claim they have implemented an Active Choice option how will we know if they have done it in accordance with the spirit as well as the letter of what was intended?

We should also establish the principle that, where an individual company declares that it has signed up to this initiative but subsequently it institutes or experiences any material change to the status quo which is likely to affect any aspect of child safety, this should be reported or made known to appropriate stakeholders in a timely manner.

For these reasons we think it will therefore be essential to establish a properly resourced independent mechanism for reassuring the public that everything that

ISPs, WiFi providers and others promised would be done was in fact done, was implemented within an appropriate timescale and on an on-going basis continues to work satisfactorily.

References to the importance of independent monitoring and review first featured in Byron, in March, 2008, but hitherto we have made well-nigh zero progress towards getting it going. Yet we have had more than one example of how the absence of an independent review mechanism may have allowed significantly unacceptable practices to continue for an unconscionably long time

Once the parameters of this area of policy are finalised and clear the Government should stay well away from any further, detailed involvement. Whenever the Government engages with issues such as these it heightens concerns in the free speech and online privacy communities, it causes anxieties about free expression. One might argue whether or not such concerns or anxieties are exaggerated or always justified but there is no getting away from the fact that such feelings exist.

As we have repeatedly stated elsewhere, we hold to the values of free speech, privacy, freedom of association and free expression as strongly as any other civil society interest group. At no point, for example, have we argued that any material which is legally available on the internet should cease to be available. Our only point is that some of it should not be so easily accessible to children. We have no desire to prevent adults from accessing adult material. That's their business not ours. Neither do we accept that the adult bar and age verification systems which we advocate would in any way compromise anyone's reasonable expectations of privacy.

Perhaps an organization such as the IMCB could be created to be an independent monitoring and review body to oversee and guarantee the integrity of these processes? It could also oversee and sign off the work of individual companies in relation to this initiative and any queries about it which might arise subsequently. Or maybe the BBFC could take this under its wing? Perhaps Reg Bailey could have a continuing role of some sort?

Lack of clarity

The language used in the consultation document to describe the three options has not helped to bring a high degree of clarity to the debate.

For example, in relation to option (a) the phrase "you can ask later" has a highly elastic meaning. It might indicate that you will be presented with information and an opportunity to enquire about it at the very next screen. However, it could imply that this will happen on the same screen, just a bit lower down, or alternatively that it might be presented at some indeterminate point in the future. These are not nit-picking details. Referring back to our earlier remarks about the concerns

of the free speech and privacy communities, they are of fundamental importance to how this initiative will be viewed and received by many important audiences.

10 b) A system where you are **automatically asked some questions** about what you want your children to be able to access on the computer or other device (including pornography, but also including things like 15-rated films, information about drugs, and whether and when you'd like them to be able to access social networking sites). There would be no answers decided for you in advance (no defaults).

☐ Yes	x No	☐ Not Sure

This seems to be the closest to the original Bailey recommendation. A lot would depend on how it is presented but it could be more confusing than option (a) and for that reason is likely to reduce the number of parents who otherwise would use it.

10 c) A **system that combines (a) and (b),** where you are asked all these wider questions in (b), but where for some obviously harmful content (like pornography), some of the answers are 'ticked' for you in advance, so that if you don't change the setting as you are going through the questions, the content is blocked. You would still be able to change the answer if you wanted to.

☐ Yes	x No	☐ Not Sure

As far as we can see the principal difference between this option and b is that a description of the adult categories are displayed on the screen “pre-ticked” i.e. turned on. This has some merit in that it acts as an immediate reminder of the sort of content or sites that the filter will address whereas, presumably, with options a and b a parent would need to click on a link or go somewhere else to see exactly what type of content would be restricted.

11 Do you think systems like this should be in place for all internet connections and households, or just for those with children?

x All households	Just households with Children

We are not out of sympathy with the idea of limiting this initiative to households that only have children but it seems to us trying to achieve that may add a layer of complexity which might be unwarranted. If that is the case then we would favour the arrangement being extended to all households. Clearly everybody would have the option to remove any and all controls but the principle should be retained that adult content should only be accessible by persons who have been verified as being 18 or above.

12 Do parents and others responsible for more vulnerable children (for example, the very young, the emotionally vulnerable, children with learning difficulties, children without responsible parents) need additional help? [Please specify]

x Yes	☐ No	☐ Not Sure

All parents need advice and support but some parents and children have specific needs requiring more focused and tailored support.

The advantage of default on or opt in is that it would deliver at least a minimum degree of protection to all households, which would include those with very young children or those who are emotionally vulnerable or have special needs. It is not obvious how that would happen if default on or opt in was not in place.

Section 4 - Education and awareness

Parents cannot properly teach their children to be safe online unless they have an understanding of the online world and what tools and techniques are open to them. Children may also get advice on keeping themselves safe online from other trusted sources: for example, their school. The following questions seek your views on how best to improve internet safety education for parents and children.

13 How do you or your children most like to get information about the safe use of the internet? [Please tick all that apply]

☐ Information sent directly by ISP, mobile phone company or other business	☐ Information in lessons at school	☐ Information from law enforcement bodies like the Child Exploitation and Online Protection Centre (CEOP)
☐ Information from charities like BeatBullying	☐ Information from the TV, newspapers, magazines, news websites	☐ Other [please specify]

All of the above. In addition we know that children and young people get a great deal of information and advice from each other. This is one of the reasons why we think putting a great deal of effort into developing awareness of the issues among children and young people as a whole is so important. Peer to peer initiatives can be very effective.

To repeat a point we made earlier, many parents or other people who are not yet regular or comfortable users of the internet will often find that paper-based resources are of more value to them and are therefore more likely to be used by them. Putting all of the safety information online for some is the same as putting it out of reach.

Partly for this reason, it is extremely important for companies selling internet connectivity or internet-enabled devices to ensure that their staff are well versed in online safety concerns and are trained in how to respond to safety questions which parents might raise at the point of purchase or later.

14 Where would you or your children be most likely to get information you can trust about being safe on line? [Please specify]

All of the above could be useful and need to be available.

15 In addition to education (for parents, children, those who work with children), what other things can be done to protect children from negative online behaviours such as cyberbullying, sexting and grooming? [Please specify]

It is important to sign post clearly where children can seek help e.g. ChildLine.

The best protection for any and every child is their own knowledge, awareness and preparedness linked to a supportive and engaged family environment. The object of policy should be to encourage such an outcome on as large a scale as possible. However, it is also important we recognise that we must not let the best be the enemy of the good and that not all children will have the same abilities or family circumstances.

No one should ever entirely delegate their parental responsibilities to a piece of software, however sophisticated it may appear to be. Moreover as a child gets older and more mature the dynamics of the parent-child relationship will change and the value of filtering and content management tools inevitably will diminish.

We know that none of the filters or content management tools currently available will work with 100% efficiency 100% of the time. But that is not a reason for refusing to countenance their use at all. The question is do they work within acceptable tolerances? We believe they do and therefore they can be particularly useful for families with younger children.

Having said that, we think it is nonetheless also very important, partly in the interests of transparency but also partly so as to encourage improvements in the software that the efficacy of filtering and content management products are regularly reviewed by an independent body and the results published.

Our understanding is that while studies of the effectiveness of filtering and content management tools carried out at EU level have shown mixed results, the tools perform better for English-speakers and are also particularly good at detecting and blocking access to pornography. Pornography is not the only issue parents care about, but it is certainly high of their list. And of course there are many families in the UK where English is not the language commonly used at home consequently that needs to be registered as a concern.

Having acknowledged technical tools will never be a complete answer, in some situations, with children in certain families, the conversations, the constructive engagement of adult and child which we all wish to encourage and facilitate will simply never take place. Any technical measures put in place may therefore provide the *only* form of protection a child has when they go on the internet.

When set against other difficulties such children might face elsewhere in their lives it is hard to know the salience of the online aspect. It is therefore hard to know how valuable or important filters and online content management tools might be to them relative to other challenges. There is no research which points in one direction or another, but we cannot wait until research has produced the answers to everything before we act. We have to use our reasonable judgement based on our current knowledge. Against that background our view

is that the use of filtering and content management tools set by default are likely to make at least some contribution towards maintaining the welfare of a child who finds himself or herself in family or care situations of this type.

As for the perpetrators of offences against children the certainty of detection is likely to be the best deterrent, linked to community resources which could help deflect potential perpetrators before they get to a point where the possibility of offending might arise.

Bullying and sexting are generally child development and child welfare issues rather than policing ones.

Thank you for taking the time to let us have your views. We do not intend to acknowledge individual responses unless you place an 'X' in the box below.

Please acknowledge this reply x

Here at the Department for Education we carry out our research on many different topics and consultations. As your views are valuable to us, would it be alright if we were to contact you again from time to time either for research or to send through consultation documents?

xYes	☐ No

All DfE public consultations are required to conform to the following criteria within the Government Code of Practice on Consultation:

Criterion 1: Formal consultation should take place at a stage when there is scope to influence the policy outcome.

Criterion 2: Consultations should normally last for at least 12 weeks with consideration given to longer timescales where feasible and sensible.

Criterion 3: Consultation documents should be clear about the consultation process, what is being proposed, the scope to influence and the expected costs and benefits of the proposals.

Criterion 4: Consultation exercises should be designed to be accessible to, and clearly targeted at, those people the exercise is intended to reach.

Criterion 5: Keeping the burden of consultation to a minimum is essential if consultations are to be effective and if consultees' buy-in to the process is to be obtained.

Criterion 6: Consultation responses should be analysed carefully and clear feedback should be provided to participants following the consultation.

Criterion 7: Officials running consultations should seek guidance in how to run an effective consultation exercise and share what they have learned from the experience.

If you have any comments on how DfE consultations are conducted, please contact Carole Edge, DfE Consultation Co-ordinator, tel: 0370 000 2288 / email: carole.edge@education.gsi.gov.uk

Thank you for taking time to respond to this consultation.

Completed questionnaires and other responses should be sent to the address shown below by 6 September 2012

Send by post to: Public Communications Unit, Department for Education, Area 1C, Castle View House, East Lane, Runcorn WA7 2GJ

Send by e-mail to:
ParentalInternetControls.CONSULTATION@education.gsi.gov.uk