

**Consultation**

**Launch Date 28 June 2012**  
**Respond by 6 September 2012**  
**Ref: Department for Education**

## **Parental Internet Controls**

Tim Loughton, Minister for Children and Families, and Lynne Featherstone, Minister for Equalities and Criminal Information are joint chairs of the executive board of the UK Council for Child Internet Safety (UKCCIS). They are writing to members of UKCCIS to seek their views and advice on parental controls. The request is to members of UKCCIS and other organisations and individuals, especially parents, who might want to respond.



**Department  
for Education**

# Parental Internet Controls

## A Consultation

**To** UKCCIS Members, Internet Service Providers, Other Organisations, Parent/Carer, Children and Young People

**Issued** 28 June 2012

**Enquiries To** 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](mailto:ParentalInternetControls.CONSULTATION@education.gsi.gov.uk)

## Contact Details

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.

### 1 Parental Controls - seeking your views

- 1.1 We are writing as joint chairs of the executive board of the UK Council for Child Internet Safety (UKCCIS) to seek your views and advice on parental controls. Our request is to members of UKCCIS and also organisations and individuals who you think might want to respond. We are therefore launching this letter and questionnaire on the Department for Education website at: [www.education.gov.uk/consultations](http://www.education.gov.uk/consultations) so that anyone can comment.

Attached is a list of questions, a glossary of terms and a short statement setting out the current position.

- 1.2 The Prime Minister spoke recently about the possibility that internet services or devices might come with a filter on as their default setting, and said that the Government should investigate that option and seek views on it. He was clear that this could only work if there was a clear prompt for the user, telling them about the settings and giving them a chance to change them. We want this questionnaire to give business, and children's and parents' organisations, the opportunity to make clear to Government what their views and concerns are and how they see their responsibilities. We want to seek views on how parents and children can become better educated about how to minimise risks when online, but also to hear about the potential for technical solutions, and what can be done to address problems such as cyber-bullying.
- 1.3 We want to engage business, charities and voluntary organisations concerned with parenting and children's safeguarding, and parents and

young people themselves, on these issues. We want to consider what approaches to online safety are currently effective, what improvements are already in development, and what more could be done. We are particularly interested in the role of providers of products and services that give access to the internet, such as manufacturers of internet-enabled devices (for example, laptops, tablets, televisions and smartphones), internet service providers, and public wifi providers.

- 1.4 Above all, we want those who take part to consider the ways in which children and young people access the internet, how best to engage parents in helping their children be safe online, and, in turn, how businesses and other agencies can most effectively support parents.

**Tim Loughton MP**  
**Parliamentary Under-**  
**Secretary of State for Children**  
**and Families**

**Lynne Featherstone MP**  
**Parliamentary Under-Secretary of**  
**State for Equalities and Criminal**  
**Information**

## 2 The Current Position

- 2.1 The internet provides children and young people with a wealth of opportunities for their entertainment, communication, education and enrichment. But there are also risks of harm, actual or potential, through the deliberate online behaviour of others, and through accidental exposure to age-inappropriate content. As children live their lives in an increasingly digital world, they need to be as aware of the risks they face in the online world as in the offline world.

- 12% of 8-11 year olds and 24% of 12-15 year olds use social networking sites to communicate with people not known to them;
- 19% of 11-16 year olds have seen potentially harmful user generated content, rising to 32% of 14-16 year old girls;
- 8% of children 11-16 have experienced bullying on the internet;
- A third of 12-15 year olds think all search engine information is truthful.[1]

---

[1] Sources: Ofcom's Children's Media Literacy Tracker 2010 and EU Kids Online II

- 2.2 These issues have been considered in depth in recent years, in reviews for the Government by Professor Tanya Byron in 2008 and 2010, which led to the creation of the UK Council for Child Internet Safety (UKCCIS), and Reg Bailey in 2011. Both reviewers were clear that parents must be given the lead in taking decisions about their children's online safety,

and that businesses and Government need to do their utmost to support parents in that role.

The Government agrees. It is parents who purchase the services and devices through which children access the internet at home, and, increasingly, outside the home through mobile phones and portable internet enabled devices such as tablets and games consoles. The basic principles of avoiding harm on the street from traffic, or from paedophiles, or in avoiding risky behaviours, apply just as much on the internet. The Government has been working with UKCCIS and its members to ensure that parents are always presented with an unavoidable choice as to whether or not they want filters and blocks installed on their internet service or internet-enabled device. This approach is often referred to as 'active choice'.

- 2.3 Since the publication of a report from the Parliamentary Inquiry into Online Child Protection, chaired by Claire Perry MP, the public debate has been framed around the apparent ease of access that children have to online pornography. The report argued that internet service providers (ISPs) should provide broadband connections into homes with filters already in place as the default setting to block access to pornography. Adults who wanted these filters removed from their service would have to tell their ISP they wished to 'opt in' to these sites.

A variation could be to combine these ideas, so that the user is clearly and unavoidably presented with a list of content types that will be blocked unless they choose to unblock them with a simple action such as removing a tick from a box. Evidence shows that giving 'default' answers like this tends to encourage more people to accept the suggested option, and most ISPs do this for things like virus protection, where there's an obvious benefit to ticking 'yes'.

- 2.4 Concerns have been raised that ISPs will hold a list of households that have decided that they want access to adult or harmful content as a result of these decisions. This system already works in the mobile phone sector without raising such concerns from customers.

The Government and UKCCIS members are aware that exposure to pornography is not the only risk that children face when using the internet. They might access websites promoting suicide, anorexia, self-harm and violence, or be the targets of online sexual grooming or bullying. No technical solution, on its own, can be 100 per cent effective in blocking age-inappropriate web content or behavioural issues, but it is right to look at the role technical solutions can play as part of a package which also includes education, awareness raising, and, if necessary, regulatory measures. The Government accepted the recommendation of the Bailey Review that the information and communication industries should develop and introduce effective parental controls, with Government regulation if industry doesn't act thoroughly and swiftly

enough.

### 3 How to Respond

- 3.1 You can respond to the consultation by completing the response form and emailing it to:  
[ParentalInternetControls.CONSULTATION@education.gsi.gov.uk](mailto:ParentalInternetControls.CONSULTATION@education.gsi.gov.uk)

or sending it by post to:

Public Communications Unit  
Department for Education  
Area 1C, Castle View House  
East Lane  
Runcorn  
WA7 2GJ.

### 4 Additional Copies

- 4.1 Additional copies are available electronically and can be downloaded from the Department for Education e-consultation website at: [www.education.gov.uk/consultations](http://www.education.gov.uk/consultations)

### 5 Plans for Making the Results Public

- 5.1 The results of the consultation and the Government's response will be published on the Department for Education e-consultation website in autumn 2012.

# Appendix 1

## 1 Glossary and Definition of Terms

- 1.1 **Active Choice:** customers are presented with an unavoidable choice or series of choices through which they consciously choose whether or not they want filters and blocks installed on their internet service or internet-enabled device. There are many ways that parental controls can be implemented. The scenarios below describe some options, and are not intended to be exhaustive:

**ISP or network level parental controls:** blocking of adult or harmful websites is performed by the ISP, preventing these sites from reaching internet-enabled devices used in the home. When signing up to a new broadband contract the customer is asked at the point of sale (e.g. over the telephone), or as part of an online purchasing process, whether they would like parental controls activated. The customer may then be presented with a list of subject categories to decide which they want to block access to. This will mean all devices that connect to that internet access point are protected. Should a device in the house be connected to an alternative unfiltered internet connection, for example, when taking a laptop or games console to a friend's house, the device will no longer be protected.

**Device level, installed by purchaser:** a parent could buy or download from the internet a parental control product (or in the case of mobile phones an 'app') to install on an existing laptop, desktop computer, mobile phone, television or other device. The parent is often required to have a little technical knowledge, but the products typically offer more functionality and are more effective at blocking harmful content accurately. Only the particular device that the software has been installed on will be protected, but that device will be protected regardless of where it connects to the internet (for example, at a friend's house).

**Device level, pre-installed by manufacturer or retailer:** a parent could buy a device from a shop or online retailer with parental control software already installed on it but not yet activated. When the parent switches on the device for the first time, they are prompted on-screen to activate the parental controls as part of the initial set up of the device. In the case of mobile phones, this could mean a parental control software 'app' is pre-installed, and when the phone is switched on the parent is asked to configure the types of internet content they want to allow access to. The parent needs less technical knowledge to install the software, but they may still need to choose the categories of harmful content that they wish to block. The device is then protected regardless of where it connects to the internet.

A variation of this could be that the shop staff could install the parental control software, acting on the customer's wishes, as a value added service in the shop.

**Parental controls on public wifi internet connections:** when a mobile device connects to a publicly available wifi connection, the provider of the service may block access to adult or other content by default as part of the terms of use of that service. Strictly speaking, is not a 'parental control' because it is not managed by the parent, but is included for completeness.

**Cyberbullying:** bullying using mobile phone texting or messaging services, email, social networking sites or any other digital communications medium.

**Default on:** see "opt in".

**Internet-enabled:** any device through which the user can access the internet.

**ISP:** internet service provider; a business or other organisation providing broadband services.

**Opt in:** where the internet service is provided with filters already in place to block access to certain websites (e.g. legal pornography), and the customer has to tell their ISP they wish to 'opt in' to these sites if they want to access them. Also known as "default on".

**Public WiFi:** an internet service in a public place, for example, a café or station, to which a mobile device such as a mobile phone, laptop, tablet, or games console can connect. The service can be provided with or without access to certain sites blocked, depending on the terms of use of that service.

**Regulation:** There are three basic ways Government could regulate this activity:

- through statutory regulation. Parliament passes a law saying something should not be allowed and gives a statutory body the job of stopping it happening and punishing those who break the rules. For example, for broadcasting, Ofcom is the statutory body established by Parliament to enforce the relevant laws;
- through co-regulation. Similar to statutory regulation, but the statutory body delegates its duty to set the rules to a body created by the industry itself. Normally the statutory body keeps oversight and imposes sanctions for any breaches of the rules when industry bodies do not want the responsibility of punishing rule breakers. Video on demand services, for example, are co-regulated by the industry body (the Authority for Television on

Demand (ATVOD), which was designated by Ofcom as the appropriate regulatory body;

- through self-regulation. In this case there is no law requiring regulation but the industry sets up its own body with its own code of rules. Normally the only sanction is the publication of a breach of the code and the withdrawal of the offending item. For example, in advertising, the industry established the Committee of Advertising Practice to write the rules that apply to non-broadcast advertising and the Advertising Standards Authority to apply those rules.

**UKCCIS:** The UK Council for Child Internet Safety (UKCCIS) brings together over 180 organisations and individuals to work together to help to keep children and young people stay safe on the internet. It was launched by the Prime Minister on 29 September 2008 and is made up of companies, government departments and agencies (including the devolved governments in Scotland, Wales and Northern Ireland), law enforcement, charities, parenting groups, academic experts and others. The Council was a recommendation in Professor Tanya Byron's report 'Safer Children in a Digital World'.

**User-generated content:** material created by an individual for their own purposes, such as photographs or video, which they upload onto social networking and other sites for other people to see.