

# Ofcom Report on Internet safety measures Internet Service Providers: Network level filtering

measures

Publication date: 22 July 2014

# About this document

This report sets out the measures put in place by the UK's four largest fixed line internet service providers (ISPs) - BT, Sky, TalkTalk and Virgin Media - to introduce a family-friendly network level filtering service, which allows the account holder to choose to block web based content that might be inappropriate for children at a network level. It describes the approach taken by each ISP to the implementation of a filtering service and the presentation of an 'unavoidable choice' to new customers whether or not to activate the filter. It is not within the remit of this report to conduct an independent assessment of the efficacy of the measures taken by the ISPs.

This followed an agreement between the Government and the four ISPs, under which the ISPs committed to offering all new internet customers a family-friendly network level filtering service by the end of December 2013. The Department for Culture, Media and Sport (DCMS) asked Ofcom to report on the measures put in place by the ISPs.

This is the second of three reports that Government asked Ofcom to produce on internet filters and online safety. The first, published in January 2014 looked at parental strategies for protection of children online reviewing Ofcom's Media Literacy research from 2012 and 2013. The final report will be published early in 2015 and will review Ofcom's Media Literacy research from 2014 on parental strategies for protection of children online.

# **Contents**

Section		Page
1	Executive Summary	1
	Background	1
	Scope of the filters	1
	Implementation of network level filtering measures	2
	Email notifications	3
	Conclusion	3
2	The scope of the filtering measures	4
	Scope of the measures – devices covered	4
	Scope of the measures – editorial categories and filter settings	4
	Editorial Categories	4
	Categorisation operations	8
3	Implementation of network level filtering measures	11
	Meeting the deadlines to implement network level filtering measures	11
	Prompts to new customers to decide whether to choose filtering	11
	Context for the new filtering services	16
	Take up	17
4	Account holder verification processes	20
5	Technical description	21
	ISP technical approaches	21
	Circumventing filters	22
Annex		Page
1	DCMS letter	23
2	Prompts - customising parental controls	25
3	Prompts – Blocking/Reporting	30
4	Editorial categories	37

#### Section 1

# **Executive Summary**

1.1 This report is the second of three requested by DCMS on family friendly network level filtering services and online safety. It reports on the measures put in place by the four major fixed line ISPs (BT, Sky, TalkTalk and Virgin Media (the ISPs)) to meet their commitments to implement family-friendly network level filtering. However, it is not within the remit of this report to conduct an independent assessment of the efficacy of the measures taken by the ISPs.

# **Background**

- 1.2 On 22 July 2013, the Prime Minister announced that the four ISPs had agreed to offer all new customers family-friendly network level filtering by the end of December 2013. Following the Prime Minister's speech, DCMS asked Ofcom to produce a series of reports on internet safety measures (see Annex 1). The first and third of these reports look at 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<sup>1</sup>. This second report focuses on the implementation of the specific policy announced by the Prime Minister.
- 1.3 DCMS asked Ofcom to report on the measures put in place by the ISPs to implement family friendly network level filtering for new customers by the end of December 2013. DCMS described the ISPs' commitment as meaning that "all new customers, on setting up their new broadband service would receive a prompt inviting them to set up family-friendly filters and that, 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".
- 1.4 Ofcom asked each ISP a standard set of questions about their approach to this commitment. All of the ISPs cooperated and following the receipt of their detailed responses, we can report on the steps they took to meet this commitment.

# Scope of the filters

- 1.5 All the ISPs have introduced network level filters to cover web-based HTML coded services such as websites or social media sites across a home's internet connected devices.
- 1.6 The filters allow a consumer to manage access in their home to a range of internet services which may include age-inappropriate content or contact risks. As would be expected from a filtering service designed to address parental concerns, there are a number of filtering categories common to all the ISPs suicide and self-harm, pornography and file sharing are covered by all the ISPs' respective classification systems, as are crime, drugs, violence and hate. Alongside the common classifications, some of the ISPs also feature supplementary categories in their filtering services, covering areas such as alcohol and tobacco, media streaming, fashion, search engines and portals.

<sup>&</sup>lt;sup>1</sup> The first of which was published on 15 January 2014 (http://stakeholders.ofcom.org.uk/binaries/internet/internet-safety-measures.pdf).

- 1.7 All of the ISPs have commissioned third parties to perform the categorisation of internet content and services: BT and Virgin employ Nominum; Sky uses Symantec, and TalkTalk uses Huawei, although Symantec was also initially involved.
- 1.8 All the ISPs confirmed that the filters would apply to "all devices in the home that connect to the internet connection". This would include WiFi connected desktops, laptops, tablets, smart phones, connected televisions and games consoles but not all internet activity may be covered by the filters - those provided by TalkTalk, BT and Virgin Media may not cover the use of apps<sup>2</sup> where they are not HTML coded. although Sky's filter will typically cover app use (see paragraph 2.3 below).
- 1.9 All of the ISPs offer some additional services alongside the network family-friendly filters, some including internet security services aimed at protecting the subscriber from issues like viruses or malware. All offer device level filtering or security software for installation on individual computers.
- 1.10 All the ISPs have provided routes for both customers and site owners for reporting potential mis-categorisation of sites – typically this may involve a review against the categorisation criteria by a team at the ISP or referral to the underlying categorisation service provider.
- 1.11 Currently, none of the ISPs' filtering services feature a process by which identified mis-categorisations are shared with other ISPs, even if these are identified within common categories shared by all ISPs. This could mean that errors identified by one ISP may persist for others. However the ISPs are all members of a UK Council for Child Internet Safety (UKCCIS) working party on over-blocking, which is a possible arena for harmonisation<sup>3</sup> (see paragraphs 2.26 to 2.37 below).

# Implementation of family friendly network level filtering measures

#### Meeting the target date for implementation of the measures

BT, Sky, and TalkTalk<sup>4</sup> were offering a network level family-friendly filtering service 1.12 allowing parents to restrict categories of online content to all new customers by the Government target of December 2013. Virgin Media did not launch its network level filter until February 2014.

### Prompts to new customers to decide whether to choose filtering

1.13 New subscribers should receive a prompt during their broadband set-up process, describing the family-friendly network level filtering service and offering them a preticked option to use the filtering service. The pre-ticked prompt should be presented to the consumer in such a way that it cannot be ignored by the consumer, who has to make an "unavoidable choice" as to whether to turn the family-friendly network level filtering on or off. The unavoidable choice approach is intended to ensure that a new broadband service cannot be activated without the subscriber making an explicit decision whether or not to use the filter. The ISPs all provided images of their prompts for new subscribers (see 3.8 below), which show that option to take up the

<sup>&</sup>lt;sup>2</sup> An app is 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.

UKCCIS brings together over 200 organisations drawn from across government, industry, law, academia and charity sector, including Ofcom, to help keep children and young people safe. The working party on over-blocking is looking at the potential for over-blocking by filters and working with ISPs on a process for handling incidences of over-blocking (which it has found to be low).

<sup>&</sup>lt;sup>4</sup> TalkTalk launched its service in May 2011.

- filter is pre-ticked, requiring the subscriber to make a decision as to whether to take up the service.
- 1.14 BT, Sky and TalkTalk said that they were presenting this unavoidable choice to 100% of their new customers by December 2013. Virgin Media said that, following the February launch of their service, around 65% of new customers were not being offered the choice of family-friendly network level filtering, primarily as a result of actions taken by installation engineers. The majority of new Virgin Media installations involve an engineer visit. Virgin Media believes that in many cases the engineer runs the broadband activation process and bypasses or ignores the filtering choice. It has recognised that this is a failure in process and indicated it is taking steps to address this gap.

### Take up of family friendly network level filters by new customers

1.15 The ISPs also reported on the proportion of new subscribers offered filtering who adopted the service. There is relative consistency on take up across the three new ISPs who launched their network level filtering option recently. TalkTalk shows a significantly higher number of new customers opting to take up the offer of network filtering. We note the range of factors that might affect subscriber behaviour, including, for example, the presence of children in the subscriber home and the extent to which parents have already adopted alternative parental controls such as device level filtering, or other approaches to secure their children's online safety.

#### **Email notifications**

- 1.16 The Government asked that the filters could only be changed by the account holder, who has to be an adult. Ofcom asked the ISPs to detail the email notification or verification system they had in place.
- 1.17 For all ISPs, the point at which filtering may first be activated is when the broadband service is being activated and subsequent changes in settings are accessible though the ISPs' password-protected account management service, to which only the account holder should have access. BT, Sky and TalkTalk indicated that set-up and changes to filter settings would all also be notified to the account holder via email. Virgin Media indicated it was not able to deliver this kind of email notification at the time it launched Web Safe, but that this would be in place by September 2014.

#### Conclusion

1 12 The ISD

1.18 The ISPs have all introduced family friendly network level filtering to new customers, although Virgin Media failed to do so by the date agreed with Government and continues to encounter issues both with coverage of all new customers and with the email verification of the set-up and settings changes.

1.19 This is the initial phase of rolling out family friendly filtering. The take up figures in this report reflect the customer's choice only after the first engagement at the point at which a new customer joins the ISP's broadband service. The ISPs are now engaged in rolling out the offer of family friendly network level filtering to reach existing customers, with a view to completing this process by the end of this year. <sup>5</sup>

<sup>&</sup>lt;sup>5</sup> Although TalkTalk launched its service in May 2011 they have indicated further activity will be undertaken during 2014 to contact existing customers.

#### Section 2

# The scope of the filtering measures

2.1 In response to questions about the nature and scope of their services, the ISPs provided information about the devices covered by the measures and the categories of content offered within the parental control settings, including options to choose different levels of protection and to customise the filter.

### Scope of the measures – devices covered

- 2.2 We asked the ISPs whether their filtering service would cover all devices and all internet activity in the home. All the ISPs confirmed that their filter would cover all devices in the home using the home's internet connection.
- 2.3 Further, all the ISPs confirmed that websites and any other internet services using standard HTTP protocols and ports were covered by the filters. BT, Virgin Media and TalkTalk acknowledged that an internet service that does not use HTTP, which would include many mobile apps, would not be covered by the filter. Sky indicated that its filter would cover some apps as well as the web browsing activity captured by the other ISPs' filtering services.

### Scope of the measures – editorial categories and filter settings

## **Editorial Categories**

### **Source of the Categories**

- 2.4 In their efforts to implement family-friendly network level filtering, all the ISPs have employed third party providers to deliver the categorisation of internet content which their filter uses. The third party providers are all well established in the field of network security and filtering. BT and Virgin Media's services are provided by Nominum, Sky's is delivered by Symantec and aggregated by Xerocole, while Huawei acts as TalkTalk's provider (although this service was originally provided by a joint venture between Huawei and Symantec).
- 2.5 The ISPs' filtering categories are based on their respective filtering provider's underlying categorisation of internet content. The ISPs consulted various constituencies in selecting from the filtering options available to them. TalkTalk based their categories on customer feedback and consultations and Sky's categories are based on customer feedback, research and consultations. BT selected their categories following market and consumer research. Virgin Media's categories were arrived at following a Virgin Media hosted industry roundtable involving a number of industry and government stakeholders.

### **Summary of the Categories**

2.6 This table summarises the different categories available.

Content	ВТ	Sky	TalkTalk	Virgin
Alcohol	✓	Х	✓	Х
Crime, violence and hate	✓	✓	filter does not explicitly cover Crime	✓
Dating	✓	✓	✓	Х
Drugs	✓	✓	✓	✓
File Sharing	✓	<b>✓</b>	✓	✓
Gambling	✓	Х	<b>√</b>	Х
Games	✓	<b>✓</b>	✓	X
Hacking	✓	✓	<b>✓</b>	✓
Nudity	✓	Х	X	X
Pornography	✓	✓	✓	✓
Sexual education	✓	Х	х	Х
Social networking	✓	✓	<b>✓</b>	Х
Suicide and self-harm	✓	✓	<b>✓</b>	✓
Tobacco	✓	Х	✓	Х

- 2.7 As can be seen from the table above, there are a number of filtering categories common to all the ISPs and others that are only covered by some of the ISPs.
- 2.8 **Alcohol, drugs and tobacco** are all covered to varying degrees across the ISPs' classification systems. **Drugs** content is covered by all ISPs (BT and Virgin Media under "Drugs", Sky under "Drugs and Criminal Skills", TalkTalk under "Drugs, Alcohol and Tobacco"). BT and TalkTalk both capture **alcohol and tobacco** within their classification systems. Sky and Virgin Media do not explicitly account for this content.
- 2.9 **Crime, violence and hate** are covered by the ISPs to varying degrees by different categories. Virgin Media's filtering system includes the separate categories of "Hate", "Violence" and "Crime" to address this content. TalkTalk's system addresses some of this content under its "Weapons and Violence" category and does not include a separate "Crime" category. Sky's main category dealing with this area is entitled "Weapons, Violence, Gore & Hate", although Sky also deals with some criminal content under its "Drugs and Criminal Skills" category. BT's "Weapons and Violence" category covers sites that encourage suicide or depict, sell, review, or describe guns or weapons but criminal activity is also captured under its "Obscene and Tasteless"

- classification, which covers sites that offer advice on how to commit illegal or criminal activities. BT also has a separate "Hate and Self Harm" category.
- 2.10 **Dating** (sites that promote networking for interpersonal relationships such as dating and marriage, for example plentymorefish.com and match.com) appears across Sky, TalkTalk and BT's respective filtering services.
- 2.11 **File sharing** sites are also addressed by the different classification systems. All the ISPs cover this content using a category entitled "File Sharing" that deals with sites used to illegally distribute software or copyrighted material. Sky covers file sharing in its broader category entitled "Anonymisers, Filesharing and Hacking".
- 2.12 **Gambling** appears across TalkTalk and BT's respective filtering services.
- 2.13 BT, Sky and TalkTalk also offer a **games** classification. However this category is not covered in Virgin Media's classification system.
- 2.14 Most of the ISPs address **hacking** with dedicated categories to this effect. Virgin Media has a "Hacking" category that deals with sites that "promote or give advice about how to gain unauthorized access to proprietary computer systems, for the purpose of stealing information". BT's "Obscene and Tasteless" category targets sites with information about "illegal manipulation of electronic devices, hacking, fraud and illegal distribution of software", while Sky's "Anonymisers, Filesharing and Hacking" category addresses hacking amongst other content. TalkTalk's filtering system does not explicitly address hacking content, although some content may be covered by the Virus Alerts element of HomeSafe.
- 2.15 **Pornographic** content is also covered by all four ISPs. Pornographic content is understood by all ISPs to cover sites that contain explicit sexual content.
- 2.16 BT's service has a **nudity** category and **sexual education** categories that are separate from the pornography category. Its nudity category covers sites that contain full or partial nudity the content blocked under this category is not necessarily of a sexual nature. BT's sexual education category is intended to prevent very young children from being exposed to sites that have a significant focus on subjects that might come up in a sex education programme.
- 2.17 **Social networking** appears across Sky, TalkTalk and BT's respective filtering services.
- 2.18 **Suicide** and **self-harm** appear across all the ISPs' filtering systems. Sky and TalkTalk both cover this content under their "Suicide and Self Harm" category, while Virgin Media's service includes two separate categories entitled "Suicide" and "Self Harm". BT's category "Hate and Self Harm" covers suicide and self-harm content.
- 2.19 In addition to the content covered above, some of the ISPs feature unique filtering categories. Sky's service is the only one to include a category for **cyberbullying** and, as noted above, a security filter aimed at preventing harm to the user through **phishing and malware**. Sky have indicated that the "Cyberbullying" category is across a relatively limited number of US "college" sites, and that in order to avoid confusion as to the extent it is possible for a filter to limit cyberbullying as a potential activity online (as it can happen on more or less any contact medium on the internet) they will integrate this limited set of sites into their "Hate" filtering category.

2.20 BT's filtering service covers a number of unique categories, alongside its "Nudity" and "Sex Education" categories. They are: "Obscene and Tasteless", "Fashion and Beauty", "Media Streaming" and "Search Engines and Portals".

### Levels of filtering and customisation

2.21 All the ISPs except Virgin Media allow customisation of the content categories operated by the filter. BT and Sky additionally offer an option to select a predetermined range of content categories. This table shows any available predetermined settings offered to the user by the ISP's filtering service, along with any levels of possible customisation offered. See Annex 2 for screenshots showing the prompts for customisation.

	ВТ	Sky	TalkTalk	Virgin Media
Pre-defined	Strict	PG	None (on or off with individual	None (on or off
300000	Moderate Light	13 18	customisation)	only)
Customisation options	All or any of 16 categories can be selected individually	All or any of 10 categories can be selected individually	All or any of 9 categories can be selected individually	No customisation possible

- 2.22 BT's Parental Controls allows parents to exercise a choice as to which categories to implement. There are three pre-defined filter levels during the activation process, namely strict, moderate and light. Nudity, gambling, weapons and violence and social networking are activated in the "moderate" and "strict" settings but not in the "light" setting. Fashion and beauty, filesharing, gaming and media streaming are only applied in the "strict" setting. Sexual education is not activated in any of the predefined settings but has to be activated in a custom set-up. Customers are also offered an option to customise the categories that are blocked. BT indicated that the filter includes a range of features, including:
  - Flexibility for parents to turn on and off on request easily, but with an account holder verification process to ensure that their settings are not easily tampered with and they are informed when settings are changed;
  - Option to set automatic filter times for specific times of day:
  - Extra protection at homework time;
  - Ability to add specific sites to either an allowed or blocked list;
  - Protection against inappropriate images returned via search engines with a specific category available blocking search engines if required – allowing parents to then add a child friendly search engine to their allowed list;
  - Ability for account holder to bypass Parental Controls from the blocked page with two options; turn off controls for one hour or always trust the site.

- 2.23 Sky's network level filter is offered as an integrated product whereby, according to the level of protection selected, either one or both of a suite of parental controls and security settings can be selected. Sky's service allows subscribers to block 10 parental control categories individually, or customers can choose a pre-determined age-based setting of PG or 13, which automatically switches those of the nine content categories included in the filter's range of operation. If the "18" option is selected, no parental control filters are switched on and only security filters are implemented. Please see Annex 2 for detail.
- 2.24 TalkTalk's HomeSafe service allows parents to block nine categories of content. Customers can customise their settings by logging into the password protected "My Account" area, which allows customers to add or remove specific categories or to block up to nine specific websites. "Homework time" allows parents to adjust the categories of sites that can be accessed at specific times of the day.
- 2.25 Virgin Media indicated that it intends to add customisable features with advanced settings in the future.

### **Categorisation operations**

2.26 We asked the ISPs to describe their processes for handling reports from users and content or service providers of **mis-categorisation** of a site or service and whether complaints and the outcomes of any reviews or appeals will be published or shared with other ISPs also providing home network filtering or otherwise made transparent.

### Reporting potential mis-categorisation

2.27 Each of the ISPs has a process for users or content owners to report potential miscategorisation of a website. This table below shows the way in which each ISP indicated reports can be made. Contact can also be made through all four ISPs' Twitter and Facebook accounts. See Annex 2 for screenshots showing the prompts.

	ВТ	Sky	TalkTalk	Virgin Media
Reporting potential mis-categorisation	Email to BT	Email to Sky or via weblink on blocked page	Report button on blocked page, via My Account or email	Online web form

- 2.28 If a BT user or content owner believes a site has been mis-categorised, they can contact <a href="mailto:categorisation@bt.com">categorisation@bt.com</a>. BT's third party supplier will undertake a review and provide a decision. If there has been mis-categorisation, the third party supplier will correct this and BT will inform the requestor. If the site is correctly categorised, the requestor is informed of the reason and has the option to add the site to their personal allowed or blocked list.
- 2.29 Sky customers can log a report using a link from the block page or by sending an email to <a href="mailto:crsupport@bskyb.com">crsupport@bskyb.com</a> as set out in Help & Support on Sky.com. Domain owners can log a report by sending an email as detailed in Contact Us on Sky.com. If a report is received by email, the sender will receive a response if that is requested. Site or domain owners can contact Sky by email to check their category or report mis-categorisation.

- 2.30 TalkTalk customers can log a report using a "report" button on the blocked page. Miscategorisation can also be reported through the My Account facility channels or via email. Content owners can request a review of their website categorisation by emailing <a href="mailto:Homesafe.classification@talktakplc.com">Homesafe.classification@talktakplc.com</a>, which is displayed prominently on the "Help" pages of the TalkTalk website under the heading "notice to website owners". TalkTalk goes through each report with its third party provider and reclassifies appropriately.
- 2.31 With the Virgin Media service, a customer or website owner can send a website reclassification request to Virgin Media via an online web form, which has a freeform text box allowing the customer or website owner to say why they believe the site should be re-classified. The form is assessed by the Internet Security Team which then submits a recommendation to the Web Safe Operational Forum. The Forum meets on a weekly basis, assesses the recommendation from the Internet Security Team and approves or rejects the request. If the request is approved, the URL is immediately added to the company level black/white list as appropriate. Decisions can also be made immediately and discussed retrospectively at the Forum.

### Publication or sharing of details of complaints, reviews and appeals about mis-categorisation

- 2.32 BT and TalkTalk have no current plans to share any complaints or the outcomes of any reviews or appeals, but all the ISPs are part of a UKCCIS sponsored working group on over-blocking which may bring forward recommendations on sharing and publishing of this information. Sky has no plans to coordinate content reviews or appeals. Virgin Media was supportive of such a process.
- 2.33 The ISPs' outcomes and decision making processes are therefore not centralised through one final arbiter or otherwise shared. This approach differs from that taken by those major mobile networks which have signed up to the "UK code of practice for the self-regulation of new forms of content on mobiles"6. These mobile service operators share a classification framework used to calibrate the filters they use to restrict access to internet content via mobile networks by those under 18. The operators use the services of the British Board of Film Classification (BBFC) as the final arbiter on appeals made by website providers against categorisation decisions made under that framework. The outcomes of such appeals are shared with all mobile service operators who are party to the code of practice<sup>8</sup>. The BBFC publishes on its website quarterly reports on all the appeals it has considered, along with the outcome of each appeal.

#### Targets for responding to reports of mis-categorisation and level of reports

- 2.34 The ISPs provided information about targets associated with their mis-categorisation processes and levels of reports from launch of the filtering services until the end of March 2104.
- 2.35 BT said that it aimed to respond to mis-categorisation cases within 72 hours and would not take longer than seven days. Sky said it did not have targets for processing mis-categorisation reports but that they were usually completed within 24 to 48 hours. TalkTalk offers customers a guide of five days to deal with reports, but

<sup>&</sup>lt;sup>6</sup> Please see http://www.mobilebroadb<u>andgroup.com/documents/mbg\_content\_code\_v2\_100609.pdf</u> for the Code of Practice.

More details of the framework described can be found at <a href="http://www.bbfc.co.uk/what-">http://www.bbfc.co.uk/what-</a> classification/mobile-content.

Those operators are currently: O2, Orange, Three, T Mobile, Virgin Media and Vodaphone.

- said that in practice the majority of reports were resolved in 24 to 48 hours. Virgin Media said its maximum response time was one week, but that change could be effected almost immediately.
- 2.36 Since the launch of its service, BT had received eight requests from content owners, of which six were re-categorised and two were correctly categorised. Sky received on average 110 reports a month from customers, of which an average of 27 was miscategorised. TalkTalk said it received on average five reports a month from site owners. Of all reports, both those from customers and site owners combined, TalkTalk indicated that only 5% had been actual cases of mis-categorisation. Virgin Media said that between launch of its service at the end of February 2014 to the end of March 2014, it received 23 queries from customers, of which 13 resulted in reclassification.
- 2.37 We noted that none of the ISPs offered a dedicated route or mechanism to allow site providers to directly check the current categorisation of their site against the ISP's filter, although email requests could be made to each ISP to ascertain if a certain site was being intentionally blocked. We also noted the length of the stated turnaround times for dealing with reports of mis-categorisation could be problematic for sites whose access by the public is crucial to their business model, although we also noted that all the ISPs indicated they believed actual turnaround would be far shorter than the times indicated.

#### Section 3

# Implementation of network level filtering measures

3.1 This section covers the extent to which the ISPs have met their commitment to Government to launch a family-friendly network level filtering service and to provide prompts asking new customers whether they wish to use the services or not, by December 2013.

# Meeting the deadlines to implement network level filtering measures

3.2 This table shows the launch date of each filtering service.

	ВТ	Sky	TalkTalk	Virgin Media
Launch date	Dec 2013	Nov 2013	May 2011	Feb 2014

- 3.3 All the ISPs, with the exception of Virgin Media, were offering a filtering service allowing parents to restrict categories of content to all new customers by December 2013. TalkTalk's HomeSafe service had been in existence for several years already and had been available to all users of the service from May 2011. Sky launched its Broadband Shield service in November 2013 and BT its BT Parental Controls in December 2013.
- 3.4 Virgin Media had not launched a network level service by the Government's deadline. It launched Web Safe in February 2014.

# Prompts to new customers to decide whether to choose filtering

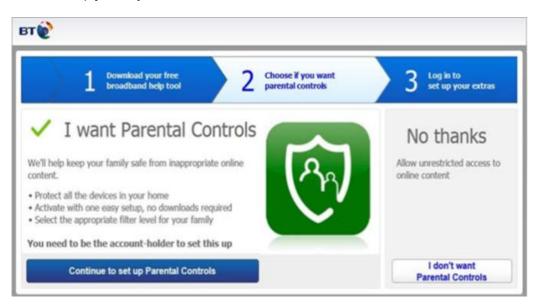
- 3.5 When Government first discussed with the major fixed line ISPs their plans to implement filters, it suggested that filters should be on if the customer "failed to engage" with the offer of the filters, for example by continuing with the subscription process without choosing whether or not to apply the filters. This suggestion was developed during discussions and the ISPs committed to offering all new customers an "unavoidable choice" whether to turn the filters on when first subscribing to the service. This should mean it would not be possible for a customer "not to engage" with the ISPs' prompts. This section covers the prompts and the implementation process to achieve that offer of unavoidable choice.
- 3.6 The table below shows the proportion of new subscribers presented with the unavoidable choice following launch of the filtering service. Details of the individual prompts offered at subscription and how they achieve that unavoidable choice then follow.

	ВТ	Sky	TalkTalk	Virgin Media
Proportion of new subscribers offered unavoidable choice	100%	100%	100%	35%

### The subscription prompts in detail

#### BT

3.7 This is the prompt presented to new BT customers as part of the BT Home Hub smart set up journey:

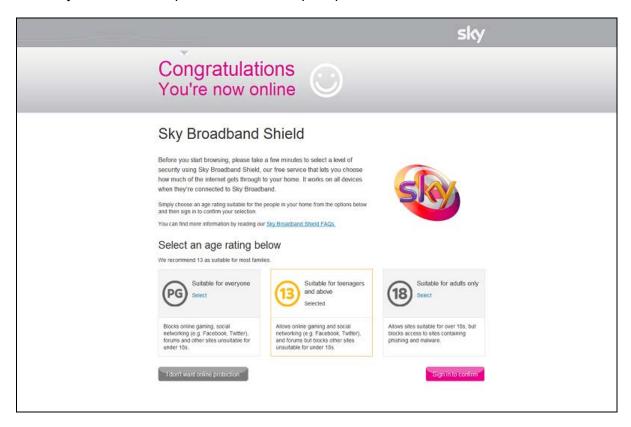


3.8 BT described the process as follows:

"The new customer is invited to choose whether to implement BT's Parental Control by means of a prompt to the new customer in the form of a pop-up window. The prompt interrupts the service activation process and the process cannot proceed without a choice being made about adoption of the filter. The prompt makes clear that the choice for the new customer is whether or not to use the BT's service-specific network level parental control filter".

### Sky

3.9 New Sky customers are presented with this prompt:

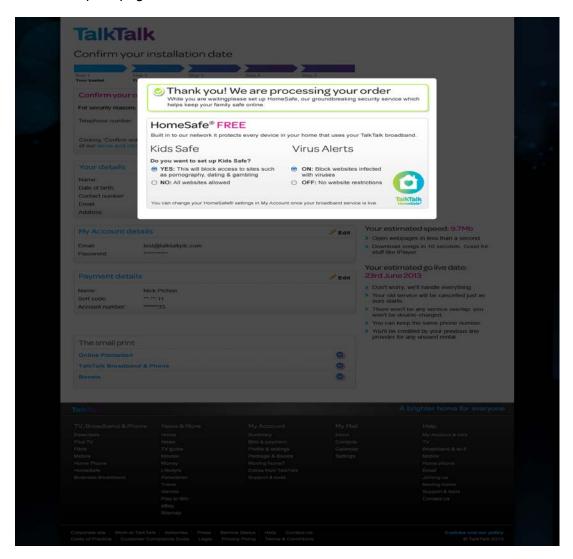


### 3.10 Sky described the process as follows:

"When customers install a new SkyHub router for the first time, regardless of whether they are a new or existing customer, are presented with a screen that invites them to choose whether to implement Sky's Broadband Shield product, and if so, to choose the appropriate preconfigured age rating. To encourage take-up the 13 age rating is pre-ticked".

### **TalkTalk**

3.11 This is the prompt given to new TalkTalk customers:

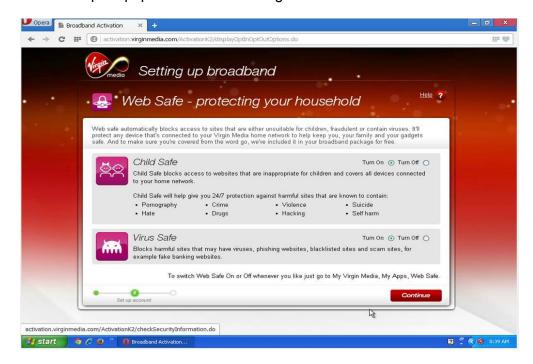


3.12 TalkTalk described the process as follows:

"The new customer is invited to choose whether to implement TalkTalk's HomeSafe by means of a prompt to the new customer in the form of a pop-up window. The prompt forms part of the sign-up process, which cannot proceed without a choice being made about adoption of the filter. The prompt makes clear that the choice for the new customer is whether or not to use the TalkTalk's service-specific network level parental control filter".

### Virgin Media

3.13 This is the prompt presented to new Virgin Media customers:



- 3.14 Virgin Media said that a new customer should be "invited to choose whether to implement Virgin Media's "Child Safe" product by means of a prompt to the new customer in the form of a page within their logged-in customer account ecosystem 'MyVM'. The prompt is part of the service activation process, which Virgin Media instructs its installers to complete with each customer. The prompt offers two products, Virgin Media's "Child Safe" product and Virgin Media's "Virus Safe" but makes clear that customer should choose whether to implement one, or both of the brand's service-specific network level parental control filter".
- 3.15 However the majority of new installations involve an engineer visit. Virgin Media understands that many engineers avoid the full broadband activation process altogether on the grounds that the process adds to the installation time. As a consequence, Virgin Media estimates that since the launch of Web Safe in February 2014, only around 35% of new customers had been presented with an unavoidable choice about implementing the filtering service. Neither Child Safe nor Virus Safe is active without the customer specifically consenting to turning the filters on.
- 3.16 Virgin Media has indicated that it understands that this fails to meet its commitment to Government and has reported that it has implemented a number of additional opportunities for the customer to see the choice and chose its network level filtering product. Virgin Media are "dramatically streamlining" the activation process so that engineers are not motivated to avoid it to save time.
- 3.17 The new prompts promoting Web Safe embedded into Virgin Media's new customer subscription journey are at the following points of contact:
  - Sales site (http://store.virginmedia.com/broadband.html);
  - Discover portal (<a href="http://store.virginmedia.com/discover/broadband/security.html">http://store.virginmedia.com/discover/broadband/security.html</a>);
  - Welcome emails (pre install);

- Install guides;
- Installer checklist;
- Post install emails;
- Quick Start IVR message; and
- Customer portal (www.myvirginmedia.com).
- 3.18 These additional prompts have resulted in additional customers finding and choosing the service. Virgin Media reported that 87% of the customers who chose their filtering service did so after activation. In Ofcom's view however these additional prompts need to be aligned with Virgin Media's development of an email notification system, to ensure that it is the account holder (i.e. the parent) that makes the decision.

## **Alternative filtering services**

- 3.19 The ISPs offer a variety of alternative filtering options, some offering device level options and some additional security options.
- 3.20 Virgin Media indicated it offers device level security with certain built in levels of parental control, through its "F-Secure Safe" system, which is available to all customers on request. These device level parental controls are currently available free of charge for the first 12 months.
- 3.21 Sky's Broadband Shield service is offered as an integrated product, whereby according to the level of protection selected, both parental controls and security settings are selected, or if preferred, if the "18" option is selected only security is offered. Sky also indicated it has device level controls available on request, a McAfee Internet Security Suite product which contains a parental control element, which is not offered at point of sale but after subscription.
- 3.22 BT Parental Controls, the network level protection, is BT's primary offering promoted to new customers as part of the subscription prompt. Once set up on the manage settings pages there is an option for BT Family Protection for customers that want to protect individual computers or laptops. Information on this is available for both new and existing customers on BT's Parental Controls product pages. BT also offers device level parental controls, with its Family Protection and Net Protect Plus options.
- 3.23 TalkTalk offers a device level product called "Super Safe Boost" which features software protection for up to five PCs and includes parental controls. The Super Safe Boost package is separate from the HomeSafe service, but is promoted as part of the welcome communication for new customers.

### Take up

3.24 This table shows the figures for take up of family friendly network level filtering by new customers who were offered it.

	ВТ	Sky	TalkTalk	Virgin Media
% of new customers who took up the offer of filtering	5% <sup>9</sup>	8%	36%	4% <sup>10</sup>

- 3.25 Each ISP provided figures on the take up of filtering by new customers **who were offered it.** These figures represent a percentage of subscribers who chose the
  <u>parental control</u> filter and reflect the customer's choice at the particular point to which
  the ISPs committed to engage with them i.e. at the point at which a new customer
  joins the ISP's broadband service. The ISPs indicated that there are additional points
  at which a customer may choose to adopt the filtering and all indicated that there was
  additional uptake at these points. Further detail on this is included at paragraph 3.31
  below.
- 3.26 TalkTalk, which launched its service in May 2011, reported significantly higher take up figures than the other three ISPs. TalkTalk said that before they introduced preticking, the number of new customers opting into HomeSafe was closer to 20%, indicating that pre-ticking had driven uptake of the service. The figures are dynamic, with customers changing their setting as family needs change.
- 3.27 There is a range of factors which will determine subscriber behaviour including, for example, the presence of children in the subscriber home and the extent to which parents have already adopted alternative parental controls such as device level filtering, or other approaches to securing their children's online safety.
- 3.28 The data does not provide any insight into the proportion of the homes offered the filters to date which have no resident children and would therefore be assumed to be less interested in parental filtering users. On a national average this would be around 40%, but this will include homes with children for whom a filtering service is irrelevant (perhaps children under 2 or 3).
- 3.29 Each ISP's demographic consumer base differs from the national average. In particular BT indicated that the figure for customers resident in homes with children was much lower and estimated that around one in four of their account holders had children from 0 to 18 years old in the household. Sky said that fewer than 40% of its customers were households with children.
- 3.30 Similarly, the data does not take into account proportion of the homes with children which are offered the filtering service but may already use alternative filtering solutions. As we set out in the Ofcom *Report* on *Internet safety measures Strategies of parental protection for children online*, on average 42% of households with children already have parental controls of some kind in place. Parents have a

<sup>10</sup> Virgin Media indicated that 13% of new customers chose a filtering option of which 100% chose Virus Safe and 33% selected Child Safe giving a figure of 4.3%.

<sup>&</sup>lt;sup>9</sup> BT indicated that 9% chose a network or device level solution, around half of whom chose a network filtering solution.

wide range of individual approaches to protecting their children, informed by their specific circumstances and preferences. Network filtering is a valuable addition to the range of parental control tools, but may not be appropriate for some parents. However, both approaches to parental controls - network or device level – can help parents manage their children's access to potentially harmful media. BT told us that around the same number of parents adopted their device-level controls as the new network-level service, suggesting that both types of service represent a valued alternative for some parents.

- 3.31 The presentation of the "unavoidable choice" may be important in raising parental awareness of filtering, and in making the adoption of filters easier for some parents. However, for all the ISPs, activation at subscription is only one of the routes by which customers can choose to activate network level filtering services. For example Virgin Media explained to us that in the three months since launching their service, they have seen large numbers of existing subscribers adopting their new filtering services independently of the unavoidable choice - particularly following the marketing around the launch of the new services – with 87% of customers that have taken Child Safe to date having done so by accessing MyVM of their own volition. Sky said they had seen more existing customers than new customers take up the filtering service. The adoption data covers only the early stages of the provision of BT, Sky and Virgin Media's filtering service and precedes marketing exercises planned by the ISPs both individually and collectively. TalkTalk's filtering service, which has run much longer than the other three services, is currently showing higher adoption among new subscribers than the other three ISPs.
- 3.32 Thus the take up figures in this report reflect the customer's choice at the particular point to which the ISPs committed to engage with them, in this initial phase of rolling out family friendly filtering. The ISPs are now engaged in rolling out the offer of family friendly network level filtering to reach existing customers, with a view to completing this process by the end of this year. Each of the ISPS indicated a variety of contact methods would be employed.
- 3.33 BT outlined that their contact strategy for existing customer's would employ email sends throughout the year to account holders, commencing in April 2014, and at relevant points throughout the year (such as with the Internet Matters<sup>11</sup> launch and then aligned to schools holiday periods). They will also employ pop-ups presented to customers logging into various BT services and browser messaging if required commencing in September 2014. BT plan various marketing activities, including the internal Update magazine sent to paper billers as well as through bt.com.
- 3.34 Age verification will be achieved through the same email approach outlined in Section 4 of this document, similar to that agreed for use with parental control offerings for new subscribers.
- 3.35 Sky indicated that their activities included an email to all existing customers on Safer Internet Day<sup>12</sup> on 11 February 2014, making them aware of Sky Broadband Shield, and asking them whether or not they wanted to use it. They also referred to an extensive marketing campaign in March 2014 across TV, radio, outside and online

18

<sup>&</sup>lt;sup>11</sup> On 13 May 2014, BT, Sky, TalkTalk and Virgin Media launched a joint campaign to promote awareness of internet safety called "Internet Matters". For more about the campaign, see <a href="http://www.internetmatters.org/">http://www.internetmatters.org/</a>

<sup>&</sup>lt;sup>12</sup> Safer Internet Day is organised by the UK Safer Internet Centre in February each year to promote the safe and responsible use of online technology and mobile phones for children and young people. More detail on Safer Internet day can be found at <a href="http://www.saferinternet.org.uk/safer-internet-day/2014">http://www.saferinternet.org.uk/safer-internet-day/2014</a>

- with characters from the Marvel Comic Book series, to raise awareness of Sky **Broadband Shield**
- 3.36 In addition, Sky indicated that when customers used their website to manage their accounts. Sky can identify which customers are yet to activate Broadband Shield. and are able to prompt them to make a choice, and do so by email.
- 3.37 TalkTalk introduced pop-ups for existing customers when they log into the "My Account" section in June 2013<sup>13</sup>. The pop-up asks customers if they wish to active the KidsSafe parental controls system, and from December 2013 TalkTalk started pre-ticking the yes box. Customers have to make a decision in response to the popup before they can access the "My Account" facility. To date, over 1.4 million existing customers have seen the pop-up and therefore made an active choice, which is broadly equivalent to the total number of customers who currently actively log in to their "My Account" section. TalkTalk are also following active plans to contact the rest of its existing customers who do not regularly use the "My Account" facility but was not in a position to update on those plans until the end of this year.
- Virgin Media's additional points of contact for existing customers and new customers 3.38 who were not offered the unavoidable choice due to the issues outlined at paragraphs 3.15 and 3.16 are included as at 3.17 above. Virgin Media indicated they had dedicated significant PR and marketing resource to raising the profile of Web Safe since launch.

<sup>&</sup>lt;sup>13</sup> TalkTalk launched its service in May 2011.

#### Section 4

# Account holder verification processes

- 4.1 We asked the ISPs what their account holder verification processes were, whether they were closed loop email and, if not, what the process was for account holder verification. Each ISP detailed their notification process, as set out below, all of which, except Virgin Media's, involve email verification of the account holder.
- 4.2 BT confirmed that to activate or change settings for BT Parental Controls, the account holder's BT ID and password were required. To ensure that someone else had not accessed the account, the account holder is sent an email each time a change is made to notify them of the changes.
- 4.3 Sky also explained that the user must sign into MySky and verify that they are the account holder or authorised person using their account or banking details.

  Activation, de-activation and settings changes are sent to the account holder by email.
- TalkTalk's initial set up is done during the sign up process for fixed line broadband, when customers are likely to be credit checked, have to provide bank details and arrange for a new broadband service to be installed or an existing service to be taken out. Customers enter into a 12 or 18 month contract, which states that customers must be aged 18 or over. Log-in details for the My Account facility, where subsequent changes to HomeSafe settings, are set up during the joining process by the account holder. The account holder can log into to My Account any time to check the status of the filtering preferences and every time a change is made to the settings an email is sent to the email address the account holder signed up with confirming the changes.
- 4.5 For Virgin Media's Web Safe only the account holder has access to the Web Safe user interface. Virgin Media indicated that they were not able to deliver email verification at the time it launched Web Safe, due to technical restrictions, but that this would be delivered in September 2014.

#### Section 5

# **Technical description**

- 5.1 This section describes the technical architecture of the filtering solutions developed by ISPs; it covers the ISPs' own operations, not the technologies used by the third parties who actually classify the content for ISPs, which are outside the scope of this report.
- 5.2 The four ISPs have quite reasonably provided Ofcom with a limited account of their individual approaches in order to keep confidential commercially sensitive details about their own network operations, and to avoid the wider distribution of information which might make it easier for the filtering system to be circumvented.
- 5.3 This section of the report is therefore limited in scope and detail but does outline the broad approaches taken by the ISPs, each of which has adopted a slightly different technical model.
- 5.4 The filtering solutions rely on two basic technologies:
  - Filtering by Uniform Resource Locator (URL) blocking: the filtering of sites or services based on their web address either addresses covering whole websites (http://www.example.com) or individual sections or pages on those sites (http://www.example.com/adultpictures). This involves the ISP checking some or all of the URLs which an opted-in subscriber requests against the list of sites or pages to be blocked. If there is a match, the subscriber request is not fulfilled typically a page with the message "this site is blocked because it is classified as..." may be delivered instead.
  - Filtering by Domain Name System (DNS) alteration: the DNS translates
    domain names ("www.example.com" into IP addresses "192.0.32.10"), to allow a
    subscriber's content request to be correctly directed this is the first stage in
    requesting a website or service. When used for filtering, the ISP's DNS server will
    not provide the IP address for domains on the list; it may instead direct the
    subscriber request to an information page with "this site is blocked because it is
    classified as...".

# ISP technical approaches

- 5.5 Each of Virgin Media, BT and TalkTalk has adopted a slightly different version of URL blocking; Sky's filtering system is exclusively based on its DNS servers. The use of URL blocking allows a more granular classification of online content and services: Sky's system will always block whole domains, while BT, Virgin Media and TalkTalk can target specific parts of a domain. In the examples above, Sky's system is capable of blocking at a domain, e.g. example.com, or a sub-domain level, e.g. domain.example.com, while the other ISPs can block parts of the site (e.g. http://www.example.com/adultpictures) while allowing other parts (e.g. (http://www.example.com/kidsgames).
- A solution based on the DNS may have benefits: for example, Sky's approach means that apps may be covered as well as standard web browsing, as apps may use the DNS even if they do not use standard web ports and protocols. The other ISPs' solutions focus on web traffic/URLs and may not capture the use of some apps (as noted above in the Scope of the measures section, from paragraph 2.2 above).

- 5.7 BT and Virgin Media informed us that they both use a two-stage process, under which the DNS system identifies potentially unwanted domains, and diverts the subscriber requests to a proxy server; the proxy server holds a more specific filtering list which may include whole domains (http://www.example.com) or selected parts of a domain (http://www.example.com/adultpictures).
- 5.8 TalkTalk provided a more limited account of their technical approach, but we believe it involves checking every URL accessed by a HomeSafe subscriber against their list of classified URLs.

## **Circumventing filters**

- 5.9 There is a broad consensus that all filtering solutions face risks of circumvention, by a dedicated and technically competent user, supported by a range of advice available online. All four ISPs provide their subscribers with advice about the complementary actions they should take, as parents, to help secure their children's online safety.
- 5.10 Although the possibility of filter circumvention remains, each ISP has taken some steps to limit the extent of circumvention. For example, ISPs include lists of "proxy sites" whose primary purpose is to bypass filters or increase user anonymity as part of their standard blocking lists. In some cases, specific adaptations have been introduced to the filtering system to maintain blocks on sites which use encryption (such as Facebook and Twitter) but to which parents wish to restrict access. However, the use of wholly encrypted connections, as is the case when a VPN 14 service is active, would bypass all selective filtering services.

## Impact on internet access

5.11 Each ISP states that the filtering service has no impact on the general quality of the internet access service opted-in subscribers receive and that they undertake continuous monitoring to ensure this is the case. The primary concern about quality noted by the ISPs was over the possibility of incorrect categorisation of sites and services; and each ISP has processes in place, described in paragraphs 2.26 to 2.37 above, address reports of incorrect filter operation.

22

<sup>&</sup>lt;sup>14</sup> A Virtual Private Network allows individuals and businesses to communicate securely over shared network infrastructure by encrypting communications traffic – as though the user was on a private network. ISPs cannot see which sites and services their subscribers are accessing when the subscriber is using a VPN.

#### Annex 1

# **DCMS** letter



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

Our Ref:

CMS 240583/DC

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

T: 020 7211 6000 P: 020 7211 6309 enquiries@culture.gsl.gov.uk www.gov.ukidoms

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:

#### 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 familyfriendly 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.

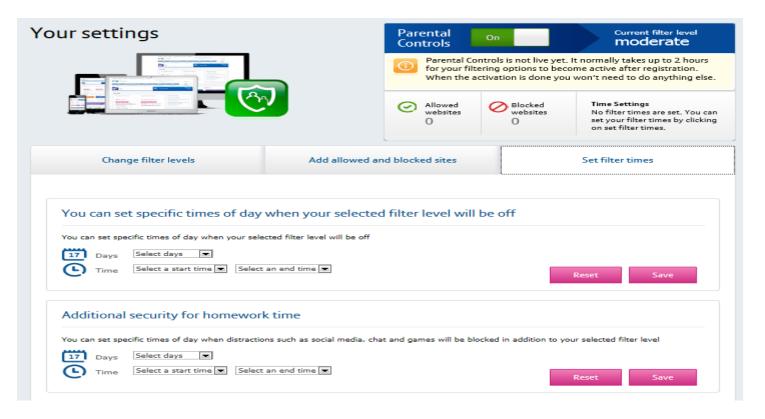
Rt Hon Maria Miller MP

Secretary of State for Culture, Media and Sport and Minister for Women and Equalities

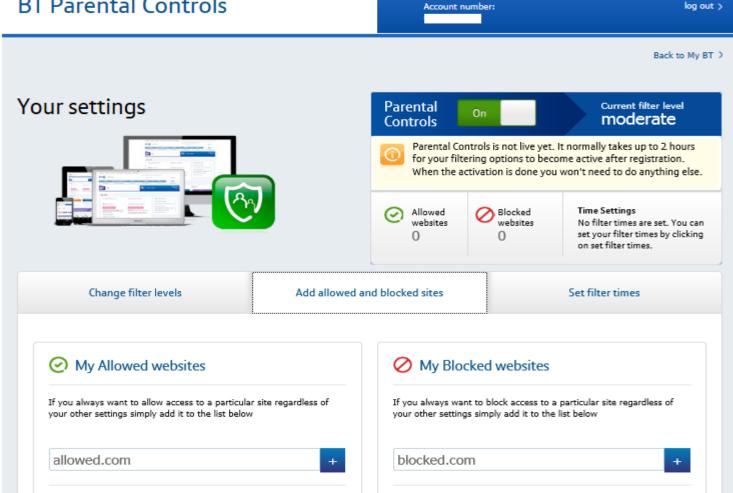
#### Annex 2

# Prompts - customising parental controls

### BT

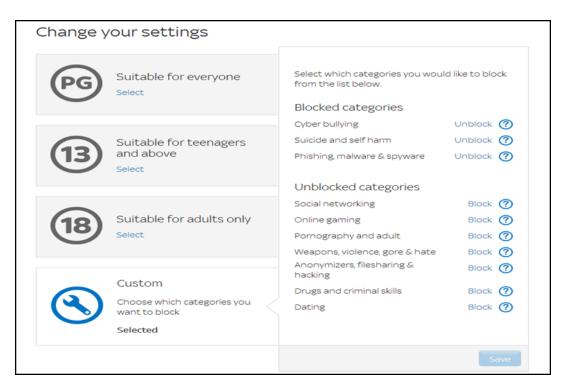


# **BT Parental Controls**



edit account )

# Sky



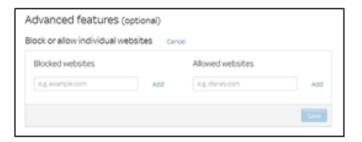
# Allow and Block Specific Web Sites

Customers can choose to block or allow specific web sites



Customers can enter the website address in the relevant box to block a web site or if allowing it will override any category block.

For example if Social Networking is blocked and the customer enters facebook.com in the Allowed web sites. The customer will then be able to access Facebook but other Social networking sites will still be blocked.



.

# TalkTalk

Choose which we	bsites to block and all	<u>low &gt;</u>	
Website categories	Specific websites		
ick the types of websites you want block.	Add websites you want to Example: www.national-lo		llow.
insuitable for under 18s		Block	Allow
Dating (i)	www.example.com		0
Drugs, Alcohol and Tobacco	www.example.com		
Gambling (i)	www.example.com		
Pornography 🕦	www.example.com		0
Suicide and Self-Harm (i)	www.example.com		0
Weapons and Violence	www.example.com		
ther types of website	www.example.com		
File Sharing Sites (1)	www.example.com		0
Games (j)	www.example.com		
Social Networking (i)			

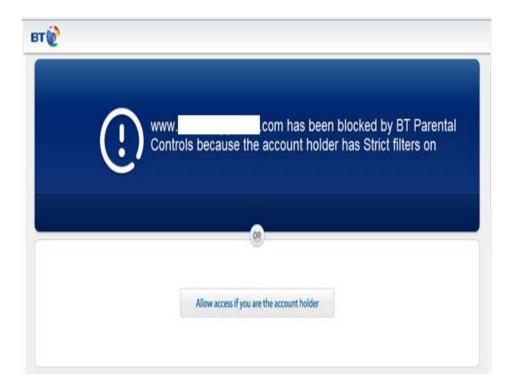
# Virgin Media

Customising is not an option at the moment

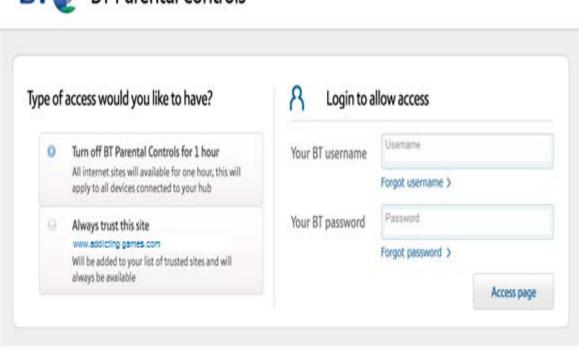
### Annex 3

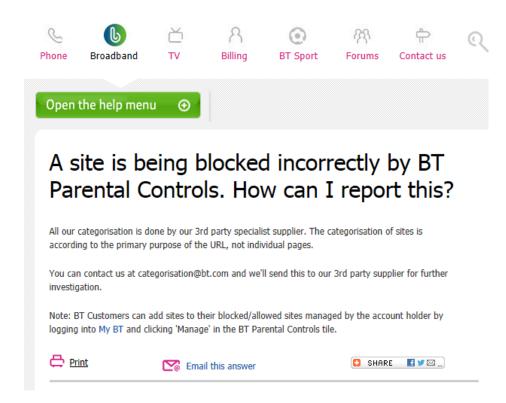
# Prompts – Blocking/Reporting

## BT



# BT Parental Controls





# Sky

# Confirmation Email sent when settings are changes and block page displayed if you try to access blocked content

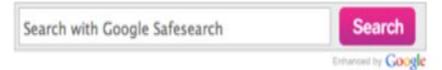




33

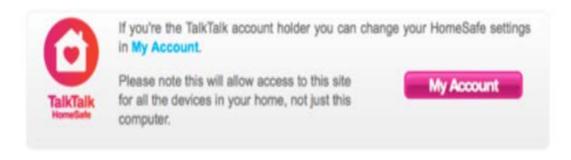
### **TalkTalk**





# Your HomeSafe settings stop you from accessing this site.

The site you tried to access was detected to contain content that falls into the category Forum, which the HomeSafe settings for your home won't allow.



If you think the site you were about to visit has been categorised incorrectly, click 'Report' to let us know.



# **Virgin Media**



# Sorry, Web Safe has blocked this site

This site has been blocked by Web Safe. It's listed as having content that's inappropriate for children, involving either pornography, hate, crime, drugs, violence or hacking.

Find out more about Web Safe Change your Web Safe settings





# Annex 4

# Editorial categories

	ВТ	Sky	TalkTalk	Virgin Media
Basis of Filter	Alcohol and Tobacco: Sites	Waanans Violanca Gara 8	Drugs, Alcohol and	Crime: Sites that offer
Settings	that promote or sell alcohol or	Weapons, Violence, Gore & Hate:	Tobacco: Sites that	advice on how to commit
Settings	tobacco related products or	Sites which sell, manufacture,	promote either the legal	illegal or criminal activities,
	service	or describe the manufacture of	or illegal use, manufacture	or to avoid detection.
	Service	weapons. Sites which promote	or distribution of drugs,	These can include how to
	Weapons and Violence: Sites	or instruct other on how to	alcohol and tobacco.	commit murder, build
	that encourage suicide or	cause property damage,	alconor and tobacco.	bombs, pick locks, etc.
	depict, sell, review or describe	physical harm or death	Weapons and	Also includes sites with
	guns and weapons. This could	through the use of homemade	Violence: Sites that	information about illegal
	be for sport or sites that contain	weapons, explosive devices,	promote violence, weapons	manipulation of electronic
	images or text depicting or	or other criminal violence.	and the infliction	devices, hacking, fraud
	advocating physical assault	Sites which display excessive	of pain.	and illegal distribution of
	against humans, animals, or	and graphic violence and/or		software.
	institutions. Sites where the	the infliction of pain or injuries	Dating: Sites which	
	content is of a particularly	towards humans or animals.	introduce people to others	Hate: Sites that promote a
	gruesome nature will be		online looking for	supremacist political
	blocked as well as sites that	Sites which advocate hostility,	relationships, for example	agenda, encouraging
	contain profanity.	aggression and the denigration	www.plentyoffish.com	oppression of people or
		of an individual or group on the	and <u>www.match.com</u>	groups of people based on
	<b>Dating</b> : Sites that promote	basis of race, religion, gender,		their race, religion, gender,
	networking for interpersonal	nationality, ethnic origin, or	File Sharing Sites: Sites	age, disability, sexual
	relationships such as dating and	other involuntary	that provide or promote	orientation or nationality.
	marriage. This includes sites	characteristics. Sites that use	file sharing applications,	\ <b>,</b> ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
	used for match-making, online	purported scientific or	for example	Violence: Sites that
	dating, spousal introduction and	commonly accredited methods	www.bittorrent.com	contain images or text
		to justify inequality,	and	depicting or advocating

escort services.

**Drugs**: Sites that give information on illegal drugs or misuse of prescription drugs.

File Sharing: Sites used to illegally distribute software or copyrighted materials such as movies, music, software cracks, illicit serial numbers, illegal license key generators and sites used as a direct exchange of files between users without dependence on a central server.

**Gambling**: Sites that offer or are related to online gambling, lottery, casinos and betting agencies involving chance.

Games: Sites relating to computer games, online games or other games. This also includes sites that provide information about game producers, or how to obtain cheat codes. This will include blocking access to online multiplayer gaming servers and online app stores.

**Pornography**: Sites that contain explicit sexual content.

aggression, and hostility.

**Dating:** Sites which promote or provide the opportunity for establishing romantic relationship.

### **Drugs and Criminal Skills:**

Sites which provide information, resources, equipment or methodology used in the commission of crimes and the avoidance of prosecution for such crimes.

Sites which promote, offer, sell, supply, encourage or otherwise advocate the recreational or illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.

# Anonymisers, Filesharing and Hacking (PG, 13): Sites which provide

Sites which provide anonymous access to websites through a PHP or CGI proxy, allowing users to gain access to websites blocked by corporate and school proxies as well as parental control filtering www.limewire.com .

Gambling: Sites where people can place bets/gamble (including lotteries), for example www.national---lottery.co.uk and www.williamhill.com.

**Games:** Sites where people can play games online, for example <a href="https://www.miniclip.com">www.miniclip.com</a> and

www.worldofwarcraft.com

**Pornography:** Sites that contain sexually explicit material.

Social Networking: Sites where people can build personal profiles and talk to others online(includes blogs, forums and virtual communities),for example www.facebook.com.

Suicide and Self Harm: Sites that promote or describe how to self harm or commit suicide. physical assault against humans, animals, or institutions; sites of a particularly gruesome nature; sites that contain profanity.

**Drugs**: Sites with information on the purchase, manufacture, and use of illegal or recreational drugs and their paraphernalia, and misuse of prescription drugs and other compounds.

Hacking: Sites that promote or give advice about how to gain unauthorized access to proprietary computer systems, for the purpose of stealing information, perpetrating fraud, creating viruses, or committing other illegal activity related to theft of digital information.

Pornography: Sites that contain explicit sexual content. Includes adult products such as sex toys, CD-ROMs, and videos,

This includes adult products such as sex toys and videos, adult and escort services, strip clubs, erotic stories and descriptions of sexual acts.

Social Networking: This category will block social networking sites used for friendship, dating, professional reasons and other various topics. It will also block sites used for online chat, like chat rooms and instant messenger sites.

Hate and Self Harm: Sites that promote or encourage self-harm or self-injury. The category also includes sites that encourage the oppression of people or groups based on their race, religion, gender, age, disability, sexual orientation or nationality.

Obscene and Tasteless: Sites that offer advice on how to commit illegal or criminal activities, or to avoid detection. These can include how to commit murder, build bombs, pick locks, etc. Sites with information about illegal manipulation of electronic devices, hacking, fraud and

solutions.

Sites which feature networks, clients and protocols related to the practice of making files and digital content available for other users to view or download including sites which offer unauthorized content for streaming, such as movies, books or TV shows.

Sites which promote or provide the means to practice illegal or unauthorized acts using computer-programming skills.

**Gaming:** Sites which are related to the development, promotion, review, and enjoyment of online, PC, and console video gaming.

### **Pornography and Adult**:

Pornography -- sites which contain explicit material for the purpose of causing sexual excitement or arousing lascivious interest.

Sex Advice -- Sites which provide information, techniques, exercises and products intended to improve the sexual lives of adults. Also

adult services such as video conferencing, escort services, and strip clubs, erotic stories and textual descriptions of sexual acts.

**Suicide**: Sites that promote, advocate or offer advice on how to commit suicide

**Self Harm**: Sites that promote, advocate or offer advice on how to self harm.

illegal distribution of software will be blocked along with content that may be offensive or tasteless such as bathroom humour, or gruesome or even frightening content such as shocking depictions of blood or wounds, or cruel animal treatment.

**Nudity**: Sites that contain full or partial nudity. The content blocked will not necessarily be of a sexual nature. This will include sites where the main purpose is to advertise or sell lingerie, intimate apparel, or swimwear.

Fashion and Beauty: Sites that relate to the advertising and discussion of fashion, jewellery, glamour, beauty, modelling, cosmetics or related products or services. This will also include sites where the main content contains fashion and beauty product reviews, comparisons, and general consumer information.

**Media Streaming**: Sites that deliver streaming content, such as Internet radio, Internet TV or music. It will also block sites

sites containing explicit or detailed discussions of sex and adult sexuality.

### **Social Networking:**

Sites which offer users the ability to chat online (by broadcasting messages to people on the same site in real time).

Sites which provide a webbased application enabling users to participate in the discussion of numerous topics.

Virtual community/social networking sites which facilitate online socializing and the development or maintenance of personal and professional relationships across geographical and organizational boundaries.

**Suicide and Self Harm:** Sites advocating or glorifying suicide as well as educating people on how to commit suicide.

Sites which advocate, normalize, or glamourize repetitive and deliberate ways to inflict non-fatal harm to oneself. that provide live or archived media downloads. Fan sites or an official site run by musicians, bands, or record labels will also be blocked.

Search Engines and Portals: Sites where the main purpose is to enable the searching of the web, newsgroups, images, directories and other online content. Includes portal and directory sites such as white/yellow pages.

**Sex Education**: This category is intended to prevent very young children from being exposed to sites that have a significant focus on subjects that might come up in a sex education programme.

**Cyberbullying:** Sites or pages where people post targeted, deliberate and slanderous or offensive content about other people with the intent to torment, threaten, humiliate or defame them.

### Phishing, Malware:

Sites where the domain was found to either contain malware or take advantage of other exploits to deliver adware, spyware or malware.

Sites that contain direct links to malware file downloads: .exe, .dll, .ocx, and others.

Sites containing characteristics of phishing techniques: transposition, misspellings, common phishkit paths, and other phishing keywords. Also includes phishing sites reported to eBay and PayPal as well as other 3rd-party phishing feeds.