

# Appropriate Monitoring for Schools

June 2016



## Provider Checklist Responses

Schools in England (and Wales) are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering”<sup>1</sup>. Furthermore, the Department for Education published the revised statutory guidance ‘Keeping Children Safe in Education’<sup>2</sup> in May 2016 (and active from 5<sup>th</sup> September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated to “ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system” however, schools will need to “be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

By completing all fields and returning to UK Safer Internet Centre ([enquiries@saferinternet.org.uk](mailto:enquiries@saferinternet.org.uk)), the aim of this document is to help monitoring providers to illustrate to schools how their particular technology system(s) meets the national defined ‘appropriate monitoring’ standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is ‘appropriate’ for them.

|                        |   |
|------------------------|---|
| Company / Organisation | Barracuda Networks  |
| Address                | Brunel House<br>Stephenson Road<br>Houndmills, Basingstoke RG21 6XR<br>United Kingdom |
| Contact details        | 01256 300100 – <a href="mailto:owheeler@barracuda.com">owheeler@barracuda.com</a>     |
| Filtering System       | Barracuda Web Security Gateway  |
| Date of assessment     | 8 <sup>th</sup> December 2016   |

System Rating response

|  |  |
|--|--|
| Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.              |  |
| Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER. |  |

<sup>1</sup> Revised Prevent Duty Guidance: for England and Wales, 2015, [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/445977/3799\\_Revised\\_Prevent\\_Duty\\_Guidance\\_England\\_Wales\\_V2-Interactive.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance_England_Wales_V2-Interactive.pdf)

<sup>2</sup> <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>



## Monitoring Content

Monitoring providers should ensure that they:

| Aspect  | Rating | Explanation  |
|---|--------|--|
| <ul style="list-style-type: none"> <li>Are IWF members</li> </ul>   |        | Barracuda Networks is a member of IWF and fully implements the most current data feed<br><a href="https://www.iwf.org.uk/members/current-members">https://www.iwf.org.uk/members/current-members</a> |
| <ul style="list-style-type: none"> <li>Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'</li> </ul> |        | Barracuda are recipients of the URL database from the Home Office and have implemented it in a form that cannot be disabled.   |

## Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

| Content  | Explanatory notes – Content that:  | Rating | Explanation   |
|----------|--|--------|---|
| Illegal  | content that is illegal, for example child abuse images and unlawful terrorist content                     |        | The Barracuda Web Security Gateway implements 95 predefined URL categories which are constantly updated. As part of this, 'Illegal Software' contains websites that provides information about or downloads of pirated software 'Criminal Activity' contains websites that provide information on how to commit illegal activities, perpetrate scams or commit fraud. 'Illegal Drugs' contains websites that provide information on the manufacturing or selling of illegal drugs or prescription drugs obtained illegally. |
| Bullying | Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others |        | The Barracuda Web Security Gateway intercepts Google Web Searches, Facebook comments, Facebook messages, Facebook Wall Posts, Twitter Tweets, Yahoo emails, and LinkedIn Chat to perform keyword analysis. It will automatically flag keyword instances using built-in (and custom) dictionaries. These dictionaries include pre-defined cyber-bullying and profanity key words.  |

|                           |  |  |  |
|---------------------------|--|--|--|
| Child Sexual Exploitation | : Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet              |  | As detailed above, the WSG will inspect content posted to common online portals for key words in predefined dictionaries including 'Adult/Pornography' key words, and 'Cyber Bullying/Profanity', 'Weapons and Violence', as well as data patterns in 'Privacy' such as a birth date and phone numbers.  |
| Discrimination            | Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity |  | The category labelled 'Intolerance and Hate' contains websites encouraging bigotry or discrimination.  |
| Drugs / Substance abuse   | displays or promotes the illegal use of drugs or substances  |  | The category labelled 'Illegal Drugs' contains websites that provide information on the manufacturing or selling of illegal drugs or prescription drugs obtained illegally.  |
| Extremism                 | promotes terrorism and terrorist ideologies, violence or intolerance   |  | The category labelled 'Violence and Terrorism' contains websites encouraging, instructing, or portraying extreme violence to people or property  |
| Pornography               | displays sexual acts or explicit images  |  | There are various categories that allow a gradation of protection. 'Pornography' contains any website that contains sexually suggestive, explicit or erotic content. 'Adult Content' contains sites that include content intended for legitimate reproductive science and sexual development educational material. And 'Nudity' contains websites containing bare images of the human body which are not suggestive or explicit. The Web Security Gateway will also inspect posts to online portals listed above, for posts containing key words contained within an 'Adult/Pornography' dictionary. |
| Self Harm                 | promotes or displays deliberate self harm  |  | While the WSG does not have a category dedicated to self-harm, suicide or eating disorders, these domains may be included in other categories. In addition, the keyword monitoring and alert   |

|          |   |  |   |
|----------|---|--|---|
|          |   |  | feature can be used to flag such incidents as well.   |
| Suicide  | Suggest the user is considering suicide                                 |  | While the WSG does not have a category dedicated to self-harm, suicide or eating disorders, these domains may be included in other categories. In addition, the keyword monitoring and alert feature can be used to flag such incidents as well.  |
| Violence | Displays or promotes the use of physical force intended to hurt or kill |  | There is a category labelled 'Violence and Terrorism' which contains websites encouraging, instructing, or portraying extreme violence to people or property. The Web Security Gateway will also inspect posts to online portals for posts containing key words contained within 'Weapons and Violence' and 'Terrorism' dictionaries. |

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

The Barracuda Web Security Gateway contains a very large local database of URLs. New requests are checked against this database for categorisation, and in the event that the URL is not present in this list, the request is passed to the Barracuda Web Categorisation Service which allows the Web Security Gateway to a much larger hosted URL database. In the event that this URL is not present in the larger cloud based database, the cloud initiates a connection to the destination website, and attempts to categorise based on the observed content. Content such as text, meta-data, links and pages following those links help us build a category automatically and on the fly, which is reported back to the Barracuda Web Filter in real time. Once a URL has been automatically categorised, it is provisionally put into the URL database, the URL categorisation team will review that in due course.

The Barracuda Web Security Gateway stores each URL as a unique record locally on the device, and each record contains source IP, username as it appears in Active Directory, full destination URL and path, the action taken as well as the MIME type and the size of the connection. Each of these is stored for up to 6 months on the Web Security Gateway. Data is removed when the data is more than 6 months old, or the appliance reaches 75% of disk capacity. If retention is required for more than 6 months, then either reports can be set up to send data out on a regular basis via SMTP or SMB/CIFS in txt, csv, pdf, or html format for long term storage, or, the Barracuda Reporting Server can be introduced to retain logs for much longer. Logs can also be streamed out to a 3rd party syslog server.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

The Barracuda Web Security Gateway provides several mechanisms for allowing either users or teaching staff, or IT administrators to override block rules which can be enabled or disabled as required.

- Some users can be deterred from browsing to content deemed inappropriate by simply providing a 'Warn' splash screen, reminding users that their browsing is tracked and logged, together with a 'Proceed' button.
- Rather than allowing the students the ability to override, the teaching staff can be given 'Temporary override' access, allowing them into a dedicated portal on the appliance which allows them the ability to make a temporary rule that allows certain content for a user, with the use of a 5-6 character code while specifying a time limit. Using this code on the users' block page allows the student to browse to the site for the time prescribed. Automatic cut off prevents abuse of this content.
- IT administrators can add URLs and URL patterns to rules either directly to the UI, or via the API.

### Monitoring System Features

How does the monitoring system meet the following principles:

| Principle  | Rating | Explanation  |
|--|--------|--|
| <ul style="list-style-type: none"> <li>• Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to</li> </ul>                       |        | The Barracuda Web Security Gateway provides an intuitive system for organising policies with a clear order of precedence ensuring that students of varying abilities and age groups are blocked or allowed appropriately   |
| <ul style="list-style-type: none"> <li>• BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (i.e. not owned by the school), how is this deployed and supported?</li> </ul> |        | The Barracuda Web Security Gateway is designed to be deployed inline as well as forward proxy. A transparent inline deployment will allow the Web Security Gateway to capture and interrogate any protocols attempting to negotiate their way out of the network without the need to deploy proxy settings. Authentication can be either set up to interrogate the user for their credentials manually, or using single-sign-on by collecting the username from the WiFi hotspot directly or from Windows NPS. |

|  |  |  |
|--|--|--|
| <ul style="list-style-type: none"> <li>Data retention –what data is stored, where and for how long</li> </ul>  |  | <p>The Barracuda Web Security Gateway stores each URL as a unique record locally on the device, and each record contains source IP, username as it appears in Active Directory, full destination URL and path, the action taken as well as the MIME type and the size of the connection. Each of these is stored for up to 6 months on the Web Security Gateway. Data is removed when the data is more than 6 months old, or the appliance reaches 75% of disk capacity. If retention is required for more than 6 months, then reports can be transferred out on a regular basis via SMTP or SMB/CIFS in txt, csv, pdf, or html format for long term storage, or, the Barracuda Reporting Server can be introduced to retain logs for much longer. Logs can also be streamed out to a 3rd party syslog server.</p> |
| <ul style="list-style-type: none"> <li>Flexibility – schools ability to amend (add or remove) keywords easily</li> </ul>   |  | <p>Key words can be added and removed from custom categories easily.</p>   |
| <ul style="list-style-type: none"> <li>Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?</li> </ul> |  | <p>Guidance to schools about common filtering policies, useful reports, and authentication schemes is provided during installation.</p>  |
| <ul style="list-style-type: none"> <li>Multiple language support – the ability for the system to manage relevant languages?</li> </ul>   |  | <p>The Barracuda URL categorization service supports a global distribution of Barracuda Web Security Gateways in over 100 countries ensuring that we have adequate coverage for content in various geographic locations and languages. In addition, the administrative interface also supports multiple languages.</p>   |

|  |  |   |
|--|--|---|
| <ul style="list-style-type: none"> <li>• Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?</li> </ul> |  | <p>Alerts are given at the top of each hour for the last 60 minutes. Each digest contains either all the triggered keywords with usernames, or the requested URLs that are deemed to be related to extreme content. These alerts are sent out via email to nominated contacts. Daily and weekly notifications are also available to ensure proactive notifications.</p> |
| <ul style="list-style-type: none"> <li>• Reporting – how alerts are recorded within the system?</li> </ul>   |  | <p>All log data is stored on the Web Security Gateway for 6 months and is available in the form of built-in historical reports and real-time logs. The data can also be exported to an external reporting server for longer retention.</p>  |

Please note below opportunities to support schools (and other settings) with their obligations around Keeping Children Safe in Education?


Barracuda Networks attempts to support schools as much as possible during the trial, setup, and on-going deployment of our products. Proactive advice on the best practices on filtering, and construction of reports is a key part of the setup process. We also draw on our experience in the education community to enhance product features and capabilities.



## PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

|           |   |
|-----------|---|
| Name      | Oliver Wheeler  |
| Position  | Sales Engineer  |
| Date      | 8 <sup>th</sup> December 2016   |
| Signature |  |

In the event of the conflict between the information contained in this document, and the information in the published data sheet, the information contained in the data sheet will govern.