

# Appropriate Filtering for Education settings



June 2020



## Filtering 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”. Furthermore, the Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ obliges schools and colleges in England 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.”

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to “have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content.”

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 filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined ‘appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Untangle, Inc
Address	25 Metro Drive Ste. 210, San Jose, CA 95110
Contact details	+1 408 598 4299
Filtering System	Untangle NG Firewall
Date of assessment	June 2, 2020

## 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.	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.	Yellow

## Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
<ul style="list-style-type: none"> <li>Are IWF members</li> </ul>		Untangle's solution OEM's (whitelists / takes as our own) the functionality provided by Webroot Inc. who have been IWF members since 2011.
<ul style="list-style-type: none"> <li>and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)</li> </ul>		NG Firewall Web Filter actively implements the IWF URL List. This type of content is filtered by utilizing the "Adult and Pornography" and "Illegal" categories which include Child Abuse images.
<ul style="list-style-type: none"> <li>Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'</li> </ul>		NG Firewall Web Filter assesses the type of content on a site and categorizes it into one of 79 categories. The "Violence" category includes sites in the CTIRU list.

## Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		This type of content is filtered by utilizing the "Hate and Racism" category for sites that contain content and language in support of hate crimes and racism such as Nazi, neo-Nazi, Ku Klux Klan, etc.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		This type of content is filtered by utilizing the following sensitive categories: "Abused Drugs" (Discussion or remedies for illegal, illicit, or abused drugs such as heroin, cocaine, or other street drugs. Information on 'legal highs' : glue sniffing, misuse of prescription drugs or abuse of other legal substances.), "Alcohol and Tobacco" (Sites that provide information on, promote, or support the sale of alcoholic beverages or tobacco products and associated paraphernalia.), "Marijuana" (Marijuana use,

			cultivation, history, culture, legal issues.) and “Illegal” (Criminal activity, how not to get caught, copyright and intellectual property violations, etc.) categories.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		This type of content is filtered by utilizing the following sensitive categories: “Illegal” (Criminal activity, how not to get caught, copyright and intellectual property violations, etc.), “Violence” (Sites that advocate violence, depictions, and methods, including game/comic violence and suicide.), “Hate and Racism” (content and language in support of hate crimes and racism such as Nazi, neo-Nazi, Ku Klux Klan, etc.), and “Weapons” (Sales, reviews, or descriptions of weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications.).
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		This type of content is filtered by utilizing the following security categories: “Proxy Avoidance and Anonymizer” (Proxy servers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring. Web-based translation sites that circumvent filtering.), “Hacking” (Illegal or questionable access to or the use of communications equipment/software. Development and distribution of programs that may allow compromise of networks and systems. Avoidance of licensing and fees for computer programs and other systems.), “Malware” (Malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, and code.), “SPAM URLs” (URLs contained in SPAM), “Phishing and Other Frauds” (Phishing, pharming, and other

			<p>sites that pose as a reputable site, usually to harvest personal information from a user. “Bot Nets” (These are URLs, typically IP addresses, which are determined to be part of a Bot network, from which network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contacts.) and “Spyware and Adware” (Spyware or Adware sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, the end user or the organization, also unsolicited advertising popups and programs that may be installed on a user’s computer.)</p>
Pornography	displays sexual acts or explicit images		<p>This type of content is filtered by utilizing the category of “Adult and Pornography” ( Sexually explicit material for the purpose of arousing a sexual or prurient interest. Adult products including sex toys, CD-ROMs, and videos. Online groups, including newsgroups and forums, that are sexually explicit in nature. Erotic stories and textual descriptions of sexual acts. Adult services including videoconferencing, escort services, and strip clubs. Sexually explicit art.)</p>
Piracy and copyright theft	includes illegal provision of copyrighted material		<p>This type of content is filtered by utilizing the category of “Illegal” (Criminal activity, how not to get caught, copyright and intellectual property violations, etc.)</p>
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		<p>This type of content is filtered by utilizing the category of “Violence” (Sites that advocate violence, depictions, and methods, including game/comic violence and suicide.)</p>
Violence	Displays or promotes the use of physical force intended to hurt or kill		<p>This type of content is filtered by utilizing the category of “Violence” (Sites that advocate violence, depictions, and</p>

			methods, including game/comic violence and suicide)
--	--	--	---

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

Untangle allows an IT administrator to configure the Web Filter app to flag and/or block URL's in 75 categories based on the Webroot classification index. Individual URLs can be added to the 'Blocked Sites' list, whilst default and custom rules allow fine-grained blocking and/or flagging based on a whole host of criteria including file extension type, mine type, server country, application control risk and productivity classification. Web Filter enables categorization of over 500 million URLs in 200 languages.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy.

IT administrators using Untangle NG Firewall can configure the data retention policy for their network. Logs can be retained for up to 366 day on the appliance, and data can be uploaded to a backup drive automatically if desired.

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

IT administrators using Untangle NG Firewall can configure which categories and/or URLs to block, flag or allow. Untangle provide a customizable dashboard, extensive real-time reporting capabilities and fine-grained controls to monitor network traffic and remediate when over-blocking is a concern. Administrators can select blocked pages and allow temporary or permanent overrides for specific users, groups or by policy. Overrides are recorded and can be audited through the Untangle NG Firewall Reports app.

### Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> <li>Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role</li> </ul>		Policies can be created within NG Firewall's Policy app based on user age, role, time of day and many other criteria. Additionally, a safe browsing option forces internet searches through a "kid-safe search engine".
<ul style="list-style-type: none"> <li>Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.</li> </ul>		IPSec and OpenVPN can be blocked. The use of various proxy services can be blocked by blocking SOCKS, Tor and by blocking the ability to surf by IP.

<ul style="list-style-type: none"> <li>Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content</li> </ul>		<p>NG Firewall has a very easy to use dashboard that gives full control over filtering and allows rules to be set up to allow, flag or block content. Groups are easily configured to allow user groups specific access based on their needs.</p>
<ul style="list-style-type: none"> <li>Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking</li> </ul>		<p>Educational establishments have full control of their Untangle NG Firewall system and are able to publish their own custom rationale that supports their own unique circumstances.</p>
<ul style="list-style-type: none"> <li>Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard</li> </ul>		<p>Untangle Command Center is a centralized management portal that can be used to share policies across multi-sites. NG Firewall provides the ability to set up different policies for different groups of users.</p>
<ul style="list-style-type: none"> <li>Identification - the filtering system should have the ability to identify users</li> </ul>		<p>Untangle NG Firewall can identify and allow access for individual users based on the policies determined by the IT administrator. Untangle NG Firewall can show reports for individual users and groups and the content they access or are blocked.</p>
<ul style="list-style-type: none"> <li>Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)</li> </ul>		<p>NG Firewall provides fine-grained control of up to 1,586 mobile and app technologies.</p>
<ul style="list-style-type: none"> <li>Multiple language support – the ability for the system to manage relevant languages</li> </ul>		<p>Untangle NG Firewall apps including Web Filter and Application Control support content in multiple languages. NG Firewall can be configured in any one of 38 languages, and block pages/blocking &amp; flagging of search terms can be customized in any language.</p>

<ul style="list-style-type: none"> <li>• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices</li> </ul>		<p>NG Firewall runs as the network gateway router, or in-line with the network gateway router. All network traffic is inspected at layer 7 using deep packet inspection.</p>
<ul style="list-style-type: none"> <li>• Reporting mechanism – the ability to report inappropriate content for access or blocking</li> </ul>		<p>An admin has the ability to block, flag or allow any content. Untangle provides a link for admins to report content they feel is not categorized correctly and request re-categorization.</p>
<ul style="list-style-type: none"> <li>• Reports – the system offers clear historical information on the websites visited by your users</li> </ul>		<p>Historical information on user online activity is available through a comprehensive Reporting app with numerous pre-built reports, plus the ability to create unlimited custom reports.</p>

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to *“consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum”*.<sup>1</sup>

Please note below opportunities to support schools (and other settings) in this regard

Untangle works directly with educational institutions to understand and meet their needs. Untangle provides guidance through case studies, white papers, infographics, wiki and forum materials. Official Untangle partners also provide significant expertise in the markets they serve. Webroot, the URL categorization technology provider to Untangle, is a member of IWF. Additionally, Webroot is the trusted endpoint security provider used by the IWF.

<sup>1</sup> <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

## 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	Heather Paunet
Position	Sr. VP, Products and Marketing
Date	June 2, 2020
Signature	