Appropriate Monitoring for Schools

June 2021

Monitoring Provider Checklist Reponses

Schools (and registered childcare providers) 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, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

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*" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's 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), 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	Untangle, Inc
Address	25 Metro Drive Ste. 210, San Jose, CA 95110
Contact details	+1 408 598 4299
Monitoring System	Untangle NG Firewall
Date of assessment	September 17, 2021

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.	

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
• Are IWF members		Untangle's solution OEM's (whitelists / takes as our own) the functionality provided by Webroot Inc. who have been IWF members since 2011.
• Utilisation of IWF URL list for the attempted access of known child abuse images		Untangle does not currently utilise the IWF Hash list.
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		NG Firewall Web Monitor 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

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		This type of content is monitored by utilizing the category of "Illegal" (Criminal activity, how not to get caught, copyright and intellectual property violations, etc.)
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		This type of content is monitored 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.)

Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		This type of content is monitored by utilizing the following sensitive categories: “Illegal” (Criminal activity, how not to get caught, copyright and intellectual property violations, etc.) and “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.)
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		This type of content is monitored by utilizing the following sensitive categories: “Hate and Racism” (content and language in support of hate crimes and racism such as Nazi, neo-Nazi, Ku Klux Klan, etc. and “Illegal” (Criminal activity, how not to get caught, copyright and intellectual property violations, etc.)
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		This type of content is monitored 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 monitored 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.).
Pornography	displays sexual acts or explicit images		This type of content is monitored 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.)
Self Harm	promotes or displays deliberate self harm		This type of content is monitored by utilizing the category of “Violence” (Sites that advocate violence, depictions, and methods, including game/comic violence and suicide.)
Suicide	Suggest the user is considering suicide		This type of content is monitored by utilizing the category of “Violence” (Sites that advocate violence, depictions, and methods, including game/comic violence and suicide.)
Violence	Displays or promotes the use of physical force intended to hurt or kill		This type of content is monitored by utilizing the category of “Violence” (Sites that advocate violence, depictions, and 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 Monitor 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 Monitor enables categorization of over 500 million URLs in 200 languages.

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 provides 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.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
• Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to. Further situations may warrant additional capability, for examples boarding schools or community based access		Policies can be created within NG Firewall's Policy app based on user age, role, time of day and many other criteria.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		Untangle NG Firewall allows administrators to set up and manage alerts directly to support their system policies.
• BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supported and how data is managed. Does it monitor beyond the school hours and location		NG Firewall provides fine-grained control of up to 1,586 mobile and app technologies. Untangle NG Firewall can identify and allow access for individual users and groups based on the policies determined by the IT administrator including mobile devices. NG Firewall monitors traffic constantly and allows users and groups appropriate access. If the network is accessed from a remote location via VPN, the traffic will be monitored and filtered according to system policies.
• Data retention –what data is stored, where is it (physically– ie cloud/school infrastructure) stored and for how long. This should also include any data backup provision		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.
● Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		Untangle NG Firewall does not require any software to be installed on devices to monitor network activity.
● Flexibility – schools ability to amend (add or remove) keywords easily		IT administrators using Untangle NG Firewall can configure which categories and/or URLs to block, flag or allow. Specific URLs can be allowed or blocked if needed.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		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.
● Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		IT Administrators are responsible for the monitoring policy for their sites. Untangle NG Firewall default Web Monitor settings for schools provide a starting point for best practices in what to flag when monitoring internet traffic.
● Multiple language support – the ability for the system to manage relevant languages?		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 & flagging of search terms can be customized in any language.
● 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?		Untangle provides the ability to customize alerts for Administrators. These alerts can be emailed to users or logged in the system for manual retrieval. There are over 30 standard reports available with the ability to customize reports for a specific need.
● Remote monitoring – with many children and staff working remotely, the ability, extent and management for the monitoring of devices (school and/or personal). Included here is the hours of operation together with the explicit awareness of users.		NG Firewall monitors traffic at all times and allows users and groups appropriate access. If the network is accessed from a remote location via VPN, the traffic will be monitored and filtered according to system policies.
● Reporting – how alerts are recorded within the system?		Alerts are logged in the system logs and retained per the administrator's data retention policy.
● Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)		Untangle monitors traffic based on search terms input by the user and/or the category of the site being accessed. Visual content on a page contributes to the category a site is classified as. Additionally, Untangle provides a Kid Safe Search setting that redirects traffic through kidzsearch.com. kidzsearch is a visual child-safe search engine and web portal

		powered by Google Custom Search with academic autocomplete that emphasizes safety for children.

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

Untangle is committed to providing robust yet flexible and easy to use tools to help protect children from internet threats. Untangle NG Firewall comes with a default installation configuration specifically for schools. This provides initial best practices for the various features of NG Firewall. Untangle continually adds features to support safe internet use for children.

Monitoring 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	September 17, 2021
Signature