Appropriate Filtering for Education settings

September 2019

Filtering Provider Checklist Reponses

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), 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	RM Education
Address	142 Eastern venue, Milton Park, Abingdon, OX14 4SB
Contact details	esafety@rm.com
Filtering System	RM SafetyNet
Date of assessment	27/11/2019

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.	

.

Illegal Online Content

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

Aspect	Rating	Explanation
• Are IWF members		Since 2004 and funding council member
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Since available
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Since 2015

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.		We manage pre-populated lists of content to encompass all categories. We use web monitoring tools to assess and categorise new websites as well as feeds from external providers. We add new sites to these central lists every night based using auto-categorisation to ensure that any new sites are automatically categorised and added.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		We manage pre-populated lists of content to encompass all categories. We use web monitoring tools to assess and categorise new websites as well as feeds from external providers. We add new sites to these central lists every night based using auto-categorisation to ensure that any new sites are automatically categorised and added.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		We manage pre-populated lists of content to encompass all categories. We use web monitoring tools to assess and categorise new websites as well as feeds from external providers. We add new sites to these central lists every night based

			using auto-categorisation to ensure that any new sites are automatically categorised and added. This is in addition to the mandatory list provided to us on behalf of the Home Office.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		We manage pre-populated lists of content to encompass all categories. We use web monitoring tools to assess and categorise new websites as well as feeds from external providers. We add new sites to these central lists every night based using auto-categorisation to ensure that any new sites are automatically categorised and added.
Pornography	displays sexual acts or explicit images		We manage pre-populated lists of content to encompass all categories. We use web monitoring tools to assess and categorise new websites as well as feeds from external providers. We add new sites to these central lists every night based using auto-categorisation to ensure that any new sites are automatically categorised and added.
Piracy and copyright theft	includes illegal provision of copyrighted material		We manage pre-populated lists of content to encompass all categories. We use web monitoring tools to assess and categorise new websites as well as feeds from external providers. We add new sites to these central lists every night based using auto-categorisation to ensure that any new sites are automatically categorised and added. We also use a mandatory list provided to us by the City of London police known as the PIPCU list that contains sites know to host and provide pirated software or content.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		We manage pre-populated lists of content to encompass all categories. We use web monitoring tools to assess and

			categorise new websites as well as feeds from external providers. We add new sites to these central lists every night based using auto-categorisation to ensure that any new sites are automatically categorised and added.
Violence	Displays or promotes the use of physical force intended to hurt or kill		We manage pre-populated lists of content to encompass all categories. We use web monitoring tools to assess and categorise new websites as well as feeds from external providers. We add new sites to these central lists every night based using auto-categorisation to ensure that any new sites are automatically categorised and added.

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

We proactively conduct thorough searches in an effort to block user access to any inappropriate material, this includes feedback from our customers as well as input from external providers. We add new sites to our lists every night, adding between 50 and 500 sites every day. However, it is important to understand that we are unable to offer a 100 per cent guarantee in providing an environment that is perceived to be 'safe' by everyone. One reason for this is the constantly changing nature and content of the World Wide Web. RM block user-access to a large number of unsuitable sites. We do this by the exclusive method, which means that when an inappropriate site is found, RM prevents user access to it. This is in contrast to the inclusive method, which restricts access to all sites, except those identified as appropriate.

Although it is impossible to identify all unsuitable sites, we still believe that the exclusive method is the most suitable Internet filtering policy. Essentially, we believe that the majority of our customers would find the inclusive method too restrictive, as the scope of acceptable sites would be too limiting and this would be against the recommendations in the Keeping Children Safe in Education guidance – recommending that schools do not overblock access to the internet.

RM SafetyNet also utilises our Active-Adapt Content Filtering technology. This technology dynamically scans individual web pages for inappropriate content as they are requested. This additional protection checks the suitability of pages that have not yet been added to an RM filter list, providing an additional safety measure which instantly adapts to unsuitable content. This can be particularly important if the content of a web page may change on a daily basis due to editable content by the public, forums or comments on web pages.

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

We retain log files for 12 months and these are accessible by customers within the admin console for the full 12 months.

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

Any activity that could be deemed as 'censorship' has been demonstrated over the years to be a very controversial issue. As the population becomes more risk-aware, we expect over the long term to be using additional mechanisms (e.g. audit logs of use within institutions) in conjunction with varying levels of filtering. As the Internet is firmly established as a global medium for business, education and entertainment medium, its value is likely to increase perpetually over the years. We suspect the issue of filtering will be with society in general for the foreseeable future, and so we all need to develop our strategies and ideas together. As this is such a difficult area we depend very heavily on user feedback to choose the right course of action and welcome comments on this policy at any time via our email address filtering@rm.com RM SafetyNet ensures that illegal content is blocked whilst also providing schools the ability to choose which pre-configured filter lists are used in conjunction with any of their own lists. We will always ensure that illegal, harmful and inappropriate content is blocked, we also believe schools have a right to choose which additional web resources are available to their users. Our active content filter looks for good words as well as bad words to ensure the context of the web page is understood, this ensures that pupils have access to sites that may contain certain words within the context of education but may be blocked by over-zealous filtering solutions.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		RM SafetyNet allows you to provision users from your active directory and this includes their Year of Entry as well as their role in the school. This allows you to create groups and apply appropriate policies for that group of users.
• 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.		RM SafetyNet is updated with VPN and proxy services within the filter lists that allow a school to block these. This list is continuously reviewed and updated to ensure that it takes into account any emerging technologies or services.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		RM SafetyNet has a very simple and intuitive interface, allowing schools to make changes themselves with just a few clicks. We also have continuously updated support pages with step by step guides as well telephone and web support.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and		Our filtering policy can be found here: https://rmsafetynet.helpdocsonline.com/rm-filtering-policy

categorisation as well as over blocking		
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		RM SafetyNet has been designed to allow multiple schools or sites to be managed from one admin console for both policy and reporting purposes. Additional filter lists can be created for all sites and be made mandatory for all sites or give the individual schools the choice as to which filter lists they choose.
• Identification - the filtering system should have the ability to identify users		Usernames are synchronised from the school's Active Directory or some cloud based directories. We also support RADIUS authentication to identify users not wireless networks. A captive portal is provided for devices/users that are not domain joined
• 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)		For apps that load content from web based cloud services these can typically be permitted or denied using standard filter rules within the SafetyNet administration interface, and we offer guidance on common URLs to block: https://rmsafetynet.helpdocsonline.com/rm-safetynet-common-url-requests-for-unfiltering
• Multiple language support – the ability for the system to manage relevant languages		Filter lists are updated with sites from around the world, including those of multiple languages. Our content filter also contains words from multiple languages. The languages that are used within RM SafetyNet are: Afrikaans Albanian Amharic Arabic Armenian Azerbaijani Basque Belarusian Bengali Bosnian Bulgarian Catalan Cebuano Chinese Chinese

		Corsican Croatian Czech Danish Dutch English Esperanto Estonian Finnish French Frisian Galician Georgian German Greek Gujarati Haitian Creole Hausa Hawaiian Hebrew Hindi Hmong Hungarian Icelandic Igbo Indonesian Irish Italian Japanese Javanese Kannada Kazakh Khmer Korean Kurdish Kyrgyz Lao Latin Latvian Lithuanian Luxembourgish Macedonian Malagasy Malay Malayalam Maltese Maori Marathi Mongolian Myanmar Nepali

		Norwegian Nyanja Pashto Persian Polish Portuguese Punjabi Romanian Russian Samoan Scots Gaelic Serbian Sesotho Shona Sindhi Sinhala Slovak Slovenian Somali Spanish Sundanese Swahili Swedish Tagalog Tajik Tamil Telugu Thai Turkish Ukrainian Urdu Uzbek Vietnamese Welsh Xhosa Yiddish Yoruba Zulu
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		RM SafetyNet is applied at a network level, allowing both proxy based and transparent filtering to ensure all devices are filtered appropriately
● Reporting mechanism – the ability to report inappropriate content for access or blocking		Reporting of inappropriate content can be done via e-mail, web chat or telephone.
● Reports – the system offers clear historical information on the websites visited by your users		RM SafetyNet provides simple reports to show top bandwidth users and users that are being blocked the most as well the ability to produce simple reports on individual users

		web history, blocked content and search terms. Email alerts can be created for individual filter lists and for search terms that may indicate a safeguarding concern.

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*".[1]

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

RM provides filtering, monitoring, CPD and workshops to assist schools with effective management of online safety issues. Our CPD consists of EPICT courses, CEOP training and teacher training. Our workshops provide interactive sessions for pupils, parents, staff and governors, helping them to understand what's acceptable online behaviour, the potential consequences and where to go for help. We can offer half day or full days which usually include an evening session with parents

[1] 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	Steve Forbes
Position	Product Manager
Date	29/11/2019
Signature