Appropriate Filtering for Education settings

June 2017

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	South West Grid for Learning Trust Ltd Also known as SWGfL, SWGfL Trust, South West Grid
Address	South West Grid for Learning Trust Ltd Belvedere House Pynes Hill Exeter EX2 5WS
Contact details	enquiries@swgfl.org.uk 0345 601 3203
Filtering System	Main solution is RM SafetyNet Plus Also Smoothwall and Lightspeed used for particular deployments
Date of assessment	27 September 2017

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		SWGfL are partners with IWF in delivering the UK Safer Internet Centre and in other projects to identify illegal online content. RM (provider of main filtering solution) are IWF members and have been since 2004. Smoothwall and Lightspeed are also IWF members.
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		All filtering solutions in place incorporate the IWF CAIC list. In addition, all SWGfL 'Schools Internet Service' core deployments include the IWF CAIC list as standard.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		All filtering solutions in place incorporate the 'police assessed list of unlawful terrorist content, produced on behalf of the Home Office'. In addition, all SWGfL 'Schools Internet Service' core deployments include 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' as standard.

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.		The following responses relate to RM SafetyNet Plus, as that as the main filtering solution deployed. However, Smoothwall and Lightspeed deployments are also fully compliant. Within RM SafetyNet Plus each of these content categories is managed through pre-populated lists of content. Web monitoring tools are used to
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting		

	malicious content		assess and categorise new websites. Inappropriate sites are added to these central lists when a user brings it to our attention. Illegal and highly inappropriate content is separated into categories which are 'always on'. Other content can be controlled at school level through an administration console.
Pornography	displays sexual acts or explicit images		
Piracy and copyright theft	includes illegal provision of copyrighted material		
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		
Violence	Displays or promotes the use of physical force intended to hurt or kill		

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

No filtering solution can claim to offer a 100% guarantee that it's operation results in a safe environment for all users. Not only are online resources changing constantly, but the use cases for certain content vary widely and mean that, although RM SafetyNet Plus includes technology to differentiate filtering policies across users and groups of users, situations will occur where content is incorrectly managed.

To work towards a better filtering provision, we proactively conduct thorough searches in an effort to block user access to any inappropriate material.

RM SafetyNet Plus also incorporates 'Active Adapt', which provides content filtering in addition to the URL filtering. This technology dynamically scans individual web pages for inappropriate content as they are requested. This additional protection checks the suitability of URLs (pages) that have not yet been added to a filter list, providing an additional safety measure which instantly adapts to unsuitable content.

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

Rather than a 'walled garden', in which content is blocked by default and allowed by exception, we allow content by default and block according to a range of analytical and investigative processes.

We also encourage local adaptation of filtering policies. Whilst the IWF CAIC list and 'police assessed list of unlawful terrorist content, produced on behalf of the Home Office' are 'always on', other categories can be adjusted by administrators within schools. URLs and search terms can also be added, to create allow or deny behaviours when they are used.

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 Plus incorporates User Based Filtering (UBF), which uses the school Active Directory to understand the user groups, and then allows different policies to be created for each.
• 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 Plus incorporates a simple, web-driven administration interface to allow schools to allow or deny specific content themselves within minutes.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Detailed guides are available within RM SafetyNet Plus, and are published separately. These include http://support.rm.com/technicalarticle.asp?cref=tec4690709 http://support.rm.com/technicalarticle.asp?cref=tec4900241
• Identification - the filtering system should have the ability to identify users		With the UBF module, each user is identified using their school network user name and assigned to the relevant group for application of any filtering policies designed for them.
• 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		RM SafetyNet Plus is designed to be highly effective and appropriate for the majority of schools. As a result, and in order to reduce costs, it is deployed as a hosted (or cloud) service, with no requirement for on-premise hardware. It is able to filter content for apps that load content from web based cloud services. These can typically be permitted or denied using standard filter rules within the RM SafetyNet administration interface, and guidance is available on common URLs to block: https://support.rm.com/technicalarticle.asp?cref=tec2602419

browser delivered content)		
• Multiple language support – the ability for the system to manage relevant languages		At present there is limited multi-language support, though this is planned for development and improvement in future releases.
• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		RM SafetyNet Plus is deployed at the network level and is not reliant on any user-level software or devices.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		RM SafetyNet Plus incorporates a simple, web-driven administration interface to allow schools to allow or deny specific content themselves within minutes. Inappropriate content can also be reported via the Service Desk or to filtering@rm.com
• Reports – the system offers clear historical information on the websites visited by your users		Through the RM SafetyNet Plus administration interface users can access a wide range of real time and historical reporting to detail the websites visited.

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

SWGfL is a leader in online safety in the UK, and increasingly across the globe. We provide a full portfolio of services, from the Schools Internet Service (incorporating the filtering solutions), to assisted monitoring services, and from training and CPD to tools and resources that help schools to improve their online safety policy and practice.

[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	PAUL HANCOCK
Position	COMMERCIAL MANAGER
Date	27 September 2017
Signature