Appropriate Filtering for Education settings

June 2020

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	Netsweeper Inc.
Address	Suite 125-126, 4100 Park Approach, Thorpe Park, Leeds, LS15 8GB, United Kingdom
Contact details	Product Manager: Chris Garstin (chris.garstin@netsweeper.com)
Filtering System	Netsweeper for Education
Date of assessment	2019-10-10

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.		Netsweeper **is a member of the IWF** in good standing, and actively works with the IWF to find and block access to CSAM material.
and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Netsweeper for Education includes the **IWF list** and can block access to the URLs on the list.
Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Netsweeper for Education includes the **CTIRU list** of terrorist content and can block access to the URLs on the 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.		Netsweeper for Education includes the "**Hate Speech**" category for blocking. This category meets the requirement for blocking "**Discrimination**" themed content.
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances		Netsweeper for Education includes the "**Marijuana**", "**Substance Abuse**" and "**Alcohol**" categories for blocking. These categories meet the requirement for blocking "**Drugs / Substance abuse**" themed content.
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance		Netsweeper for Education includes the "**Terrorism**", "**Violence**", "**Extreme**", and "**CTIRU**" categories for blocking. These categories meet the requirement for blocking "**Extremism**" themed content.
Malware / Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Netsweeper for Education includes the "**Infected Host**", "**Viruses**", "**Phishing**", "**Malware**", "**Criminal Skills**", and "**Malware Hosts**" categories for blocking. These categories meet the requirement for blocking "**Malware / Hacking**" themed content.

Pornography	Displays sexual acts or explicit images		Netsweeper for Education includes the "**Pornography**", "**Nudity**" categories for blocking. These categories meet the requirement for blocking "**Pornography**" themed content.
Piracy and copyright theft	Includes illegal provision of copyrighted material		Netsweeper for Education includes the "**PIPCU**" (Police Intellectual Property Crime Unit) and "**Copyright Infringement**" categories for blocking. These category meets the requirement for blocking "**Piracy and copyright theft**" themed content.
Self Harm	promotes or displays deliberate self-harm (including suicide and eating disorders)		Netsweeper for Education includes the "**Self Harm**" category for blocking. This category meets the requirement for blocking "**Self Harm**" themed content.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Netsweeper for Education includes the "**Extreme**", and "**Weapons**" categories for blocking. These categories meet the requirement for blocking "**Violence**" themed content.

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

In addition to the categories outlines above, in the context of meeting the Appropriate Filtering standard, Netsweeper provides 90+ content categories that can be used to tailor filtering for the specific needs of each school and classroom.

Additional features such as safe-search enforcement, search keyword detection, and highly customisable URL list features provide system operators with a highly granular solution for protecting children online.

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

The Netsweeper for Education solution includes a highly configurable logging and reporting system that can be adjusted to meet regional requirements with respect to data retention.

Netsweeper recommends storing log file data for 3 years or more.

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

All Netsweeper solutions utilise the Netsweeper Category Name Service (CNS). CNS is a globally available system that dynamically categorises web content into 90+ categories and multiple languages. This system is reviewed and trained continually by the Netsweeper Content team. Additionally, Netsweeper includes "URL Alert" functionality, which provides all system operators the ability to submit URL's that have been incorrectly categorised for review.

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		Netsweeper for Education supports highly granular web filtering policies that are defined by age group, classroom, and any other parameters.
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.		Netsweeper for Education supports categories that block web-based filtering circumvention techniques (i.e.: Web Proxies, Remote Access Tools, etc.). The solution also includes protocol filtering capabilities to block known and unknown protocols, as well as firewalling capabilities to prevent filtering circumvention.
Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Netsweeper for Education includes the WebAdmin, a comprehensive management interface that places control in the hands of the system operator. Multi-tenant capabilities can be used to enable per-school, per-teacher management of the solution.
Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Netsweeper provides comprehensive documentation through an online help portal. This documentation outlines how categorisation works, category definitions, how URL's are processed, and how URL alerts can be used to identify incorrectly blocked content.
Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Netsweeper for Education includes comprehensive multi-tenant capabilities and is highly scalable to support many schools operating on a single platform. Each school is "siloed" within their own operational environment.

Identification - the filtering system should have the ability to identify users		Netsweeper for Education includes per-user filtering, including support for directory synchronisation with many leading directory services.
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)		Netsweeper for Education includes "**Web App**" and "**Mobile App**" categories that specifically target unconventional web traffic. Additionally, the solution can identify and block non-HTTP/HTTPS protocols. Netsweeper has a proactive approach to blocking and works with our customers to identify and add further protocols to the blocking capabilities within the solution.
Multiple language support – the ability for the system to manage relevant languages		Netsweeper for Education performs dynamic categorisation in 47 languages and across 90 categories. Please see: https://www.netsweeper.com/live-stats/ The Netsweeper WebAdmin interface is also available in other languages.
Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		Netsweeper for Education is a network-based solution. Client software are used to extend filtering to devices that leave the network.
Reporting mechanism – the ability to report inappropriate content for access or blocking		Netsweeper for Education includes a fully customisable reporting framework. Reports can be created on demand or scheduled. Report alerts are configured to notify administrators of incidents of concern (i.e.: Prevent, Safeguarding, etc.)
Reports – the system offers clear historical information on the websites visited by your users		Netsweeper for Education includes a fully customisable reporting framework. The reporting framework uses the URL Request Log files, which contain information on every URL request that the Netsweeper solution processed.

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

Netsweeper for Education includes functionality for placing category-specific content onto block pages. This is a meaningful way to engage with students that are encountering harmful material. Attempts to access self-harm material can take the student to resources that provide assistance. Attempts to access violent or hateful material can direct students to resources regarding inclusivity and tolerance.

[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	Chris Garstin
Position	Product Manager
Date	2020-06-04
Signature