Appropriate Filtering for Education Settings

June 2016

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*"[1]. Furthermore, the Department for Education published the revised statutory guidance 'Keeping Children Safe in Education'[2] in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated 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*."

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	Warrington Borough Council
Address	Quattro Towers , Buttermarket Street , Warrington
Contact details	
Filtering System	Fortiguard Web Content Filtering
Date of assessment	25/11/16

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.	

.

[1] Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

[2] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Illegal Online Content

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

Aspect	Rating	WBC Explanation
• Are IWF members		Fortinet is a member of the IWF
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		The IWF CAIC list is part of Fortiguard Web Filtering Service. Category – Child Abuse: websites that have been verified by the Internet Watch Foundation to contain or distribute images of non-adult children that are depicted in a state of abuse. Information on the Internet Watch Foundation is available at http://www.iwf.org.uk/
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		The list is part of Fortiguard Web Filtering Service.

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	WBC Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		**Category - Discrimination** Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group. ***Sites in this category are blocked by default for schools***
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		**Category - Drug Abuse** Websites that feature information on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc. ***Sites in this category are blocked by default for schools***
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		**Category - Extremist Groups** Sites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs ***Sites in this category are blocked by default for schools***

Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		**Category - Malicious Websites** Sites that host software that is covertly downloaded to a user's machine to collect information and monitor user activity, and sites that are infected with destructive or malicious software, specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent, such as virus or trojan horse. **Category - Hacking** Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites. ***Sites in these categories are blocked by default for schools***
Pornography	displays sexual acts or explicit images		**Category - Pornography** Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite. **Category - Nudity and Risque** Mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse ***Sites in these categories are blocked by default for schools***
Piracy and copyright theft	includes illegal provision of copyrighted material		**Category - Peer-to-Peer File Sharing** Websites that allow users to share files and data storage between each other. ***Sites in this category are blocked by default for schools***
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		**Category - Explicit Violence** This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc ***Sites in this category are blocked by default for schools***
Violence	Displays or promotes the use of physical force intended to hurt or kill		**Category - Explicit Violence** This category includes sites that depict offensive material on brutality, death, cruelty, acts of

			abuse, mutilation, etc. ***Sites in this category are blocked by default for schools***

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

The following web link contains descriptions of Fortinet's normal categories:
http://www.fortiguard.com/webfilter

FortiGuard URL Database Categories are based upon the Web content viewing suitability of three major groups of customers: enterprises, schools, and home/families. They also take into account customer requirements for Internet management. The categories are defined to be easily manageable and patterned to industry standards.

Each category contains websites or web pages that have been assigned based on their dominant Web content. A website or webpage is categorized into a specific category that is likely to be blocked according to its content. When a website contains elements in different categories, web pages on the site are separately categorized.

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

The policies which we use for schools have been carefully tailored to enable access to the majority of appropriate websites. On the occasion where a school is unable to access a specific website, the school is able to either unblock the website themselves if they have requested this level of access or contact our service desk to request the site be unblocked.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	WBC Explanation
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		Policies can be adjusted to account for different, requirements, use groups, times of day etc.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		All schools have the option of managing their own Block and Permit policies.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		The general categories are published on Fortinet's web site: http://www.fortiguard.com/webfilter
• Identification - the filtering system should have the ability to identify users		Users are identified via IP address.
• Mobile and App content – isn't limited to		The Fortinet service is in-line with

filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies		our internet feed so all internet data both egress and ingress passes through the filter.
● Multiple language support – the ability for the system to manage relevant languages		The Fortinet web filtering system has multi-language allowing effective filtering to occur regardless of the language the user is using or the page being visited.
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		No clients or agents are required on any endpoint to ensure the filtering is enforced
● Reporting mechanism – the ability to report inappropriate content for access or blocking		We implement a standard block page, and schools can either unblock or report the issue to us via our service desk for the site to be unblocked Where inappropriate access has occurred, again the school can block this site if they have requested that level of access, or contact our service desk for the site to be blocked.
● Reports – the system offers clear historical information on the websites visited by your users		The system offers a broad range of reports which schools can request. Historical data is stored for a set period of time and reports ran against this data.

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*".[3]

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

Support can be accessed from Warrington Borough Council's ICT Team or the Education Safeguarding Team.

[3] 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	David Gallear
Position	Networks Technical Lead
Date	25/11/2016
Signature	