

St Peters C of E Junior School

Keeping Children Safe

Internet Safety

The Web Filtering service (Surf Protect), provides safe, filtered and logged web access for both staff and students for the school's broadband connection. This service is an integral feature of our Broadband and Online Service Bundle.

It provides the school with the peace of mind that all filtering services are managed in the correct manner and all stake holders are kept safe. The service includes:

- Education focused web filtering
- Different filtering policies based on username, group membership or IP range
- Local control to allow the school to manage which websites and categories of websites it wishes to allow or block.
- Monitoring and reporting on web access
- Meets the DfE recommendations for web filtering to protect pupils online and the standards for schools' web filtering set by the UK Safe Internet centre.
- Illegal content (as listed on the Internet watch Foundation) remains blocked at all times and access cannot be over-ridden by school staff

What are the benefits?

- The school are able to request granular filtering themselves based on their own classroom or user needs.
- The School do not require any filtering equipment to be installed in school with this service
- Assists schools in fulfilling their safeguarding duties through the use of monitoring and reports

Web Filtering

- The filtering service is centrally hosted and managed, in addition to being locally managed. It provides safe internet access for the school managing all web traffic from Surf Protects broadband connected schools, Surf Protect Filtering blocks all sites on the Internet Watch Foundation (IWF) CAIC list.
- Surf Protect filtering implements the Home Office Terrorism Block list managing all web traffic for all connected schools, Surf Protect Filtering blocks all sites on the Internet Watch Foundation (IWF) CAIC list. Surf Protect filtering implements the Home Office Terrorism Block list

Global Filtering (All schools –default setting)

Surf Protect have initially assigned a default filtering set based on school type (Nursery/Primary/Secondary etc.), which should meet most schools' needs. The school can then choose to tailor this to the individual requirements.

The Surf Protect system features categories where there is an "Enforced Block" (these categories cannot be overridden by schools in the local settings). These are as follows:

- Pornography
- Child Sexual Abuse
- Criminal Skills
- Extreme
- Hate Speech
- Weapons
- Viruses
- Child Erotica
- Gambling
- Intimate Apparel
- Marijuana
- Substance Abuse
- Malformed URL
- Copyright Infringement
- Malicious Web Obfuscation
- Malware
- Phishing
- Web Proxy

Custom Report: This report has been created to give you more freedom to create custom reports. You are able to use this to create the own report along with customising most of the settings.

- **Suspicious Search Report:** This report lists all of the search queries which are identified by our Suspicious Search Keywords Shared List.
- **User Inspection Report:** This report shows all traffic from a particular User, this can be used to further investigate if a User has been highlighted as attempting to access content.
- **Custom Report:** This report has been created to give you more freedom to create custom reports. You are able to use this to create the own report along with customising most of the settings.

Reporting and Alerting Capabilities

Surf Protect can configure and schedule reports of internet usage. These can be exported for further analysis e.g.

- **Search Query Report:** This report lists all of the search queries from the site, this will list things like Google searches.
- **Prevent Report – Websites:** This report lists all of the websites which have been accessed which would fall under a Category which is contained within UK Prevent.

- Suspicious Search Report: This report lists all of the search queries which are identified by our Suspicious Search Keywords Shared List.
- Suspicious Search Report: This report lists all of the search queries which are identified by our Suspicious Search Keywords Shared List.
- User Inspection Report: This report shows all traffic from a particular User, this can be used to further investigate if a User has been highlighted as attempting to access content.
- Custom Report: This report has been created to give you more freedom to create custom reports. You are able to use this to create the own report along with customising most of the settings.

Filtering

- The service gives the school more flexibility when setting filtering to suit their needs. The school has the ability to request to block or unblock individual websites or categories.
- Filtering can be based on IP address ranges, individual IP addresses or by using directory services such as active directory.
- Certain websites, including illegal sites or categories of websites classed as inappropriate by the Surf Protect Filtering service, are blocked at a global level, ensuring protection for pupils and staff. All other categories are available for the school to select as either allow or block.
- This service may require the technical support staff to configure services locally. In view of the levels of flexibility offered with the Web Filtering service, the school has full responsibility for managing access to websites and to ensure that staff, pupils and guests can only access appropriate content using either a school device or personal device on the network.

Managed Service

This is a centrally managed service with management of filtering.

- Surf Protect manages all central filtering infrastructure for schools including future investment, upgrades and supplier management.
- Filters both HTTP and HTTPS (with appropriate certificate) web traffic, ensuring that pupils are protected.
- Traffic to/from certain sites such as NHS and financial services will not be decrypted by default.

As an extra measure:

The school have investigated on-site monitoring software this can be an extra instrument in our safeguarding toolbox: for instance, the Keyword and Phrase Monitoring feature provides you with an insight into what pupils are typing or searching for – and even tracks the applications used for extra context. Severity levels allocated to safeguarding keywords dictate the outcome on matching: from a simple recording of the activity in the system, through to an instant alert or screen capture. Additional details of the triggered event can also be viewed, such as the pupil's logon ID, the PC used and the time it was triggered.

The school can then print, save, email or take a screen grab of the results to forward to a colleague to follow up on – or, alternatively, if not a real concern, simply mark the event as a false alarm.

The triggered keywords and phrases within all of the safeguarding categories can also be displayed as a word count. This provides further insight into what safeguarding issues are trending at your school, enabling you to monitor and intervene where needed, even drilling down to see trends by year group for any given period of time.

The Report a Concern tool also allows students to proactively report an issue to a nominated member of staff, encouraging dialogue when support is needed. Concerns, supporting documents and history of steps are all securely recorded. The software includes all the reports and evidence to demonstrate on inspection the effectiveness of your safeguarding and Prevent policies

To safeguard the whole school community, we also provide the following:

- Staff safeguard training
- Staff filtering rules in place
- Pupils e-safety training
- e-safety training for parents

It is important to recognise that no filtering systems can be 100% effective and needs to be supported with good teaching and learning practice as well as effective supervision.

Key Features

Cloud Filtering

As SurfProtect is located entirely in the cloud, there is no need for a device to be installed at your school's site. To change your settings in any way, or to implement advanced filtering features, all you have to do is login to your web portal!

Identification

Offering a number of different ways to implement user filtering policies, SurfProtect allows you to filter by external or internal IP address or - as full AD integration is provided - by username or group policy,

HTTPS Filtering

SurfProtect is able to perform decryption of all secure traffic and, as a result, can completely filter HTTPS websites - preventing students from entering inappropriate search terms, and enabling filtering of URL paths.

BYOD Filtering

It is possible to ensure that every device receives the same level of protection. This is because network-level filtering is implemented, so all traffic on the school's connection is filtered - regardless of the device used to access it.

Online Analytics

SurfProtect provides you with an insight into the activity taking place on your school's internet connection - from which sites are being requested, which search terms are being entered and even which users are attempting to access which sites.

Downloadable Reports

With SurfProtect you are able to download reports of all online activity performed on your network. Compiled and stored over three month periods, this data provides you with a detailed insight into your school's web traffic.

Search Term Filtering

Block specific search terms, enforce SafeSearch on Google, view a live dashboard of users' searches, as well as a record of allowed and blocked search terms, including the reason they were rejected and by whom they were requested.

Application Support

Prevent your students using mobile applications to access restricted sites, such as Twitter, by blocking the chosen app/s in your portal.

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		Yes we are IWF members
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		We actively implement the IWF URL list to block access to illegal child abuse images

Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		We have integrated the police assessed list of unlawful terrorist content produced on behalf of the Home Office
Confirm that filters for illegal content cannot be disabled by the school		Filters for illegal content cannot be disabled by the school

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.		Please see below wording under the table which explains how content is managed through our filtering system.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Please see below wording under the table which explains how content is managed through our filtering system.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Please see below wording under the table which explains how content is managed through our filtering system.
Gambling	Enables gambling		Please see below wording under the table which explains how content is managed through our filtering system.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Please see below wording under the table which explains how content is managed through our filtering system.
Pornography	displays sexual acts or explicit images		Please see below wording under the table which explains how content is managed through our filtering system.
Piracy and copyright theft	includes illegal provision of copyrighted material		Please see below wording under the table which explains how content is managed through our filtering system.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Please see below wording under the table which explains how content is managed through our filtering system.

Violence	Displays or promotes the use of physical force intended to hurt or kill		Please see below wording under the table which explains how content is managed through our filtering system.
----------	---	--	--

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

Key word filtering is used to identify a search query through the use of search engines. Exa provides a curated key word list to all customers as a default, customers can then add their own additional words/sites for anything else they want to block.

When a website is visited for the first time Exa will categorise the website, for all these content types we will automatically block them. For any others the schools can choose to block. Exa will periodically sample the list to see if the content needs to remain on the blocked list.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained.

As specified in the contracts for SurfProtect, if customers have SurfProtect Quantum logs are guaranteed to be kept for 3 months, and with SurfProtect Quantum+ are guaranteed to be kept for 1 year.

The identification data held is dependent on what each customer sets usernames up as (eg if the school uses first name and last name, or student ID numbers etc. we will have that information). Data is only accessible internally to Exa by authorised personnel who need it for their job roles.

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

Exa have a default set up for customer profiles which has lists of content already blocked. Individual customers can then tailor the lists to their own needs, enabling and disabling content as required with the exception of the illegal content as mentioned at the start of this question set, this content is unable to have the filter removed.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
Context appropriate differentiated filtering, based on age, vulnerability and risk of harm		Exa provide default profiles as a standard set up,
also includes the ability to vary filtering strength appropriate for staff		customers can then create different user groups and filter by levels as required

• 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.		We can filter DNS over HTTPS VPN/Proxy is being worked on, plans are being made for how we can filter. We do filter embedded URLs to determine if they include something which should be blocked. We also can use advance firewall traffic detection to block traffic profiles such as VPN should the customers take our firewall product.
• Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes		Exa provide default profiles as a standard set up, customers can then create different user groups and filter by levels as required. Audit logs are kept for who has made changes. Schools can only make changes to their own profiles.
• Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include AI generated content. For example, being able to contextually analyse text on a page and dynamically filter.		We do this on searches on the first time a search is made, then as and when they come up as part of the sampling reviews. We would filter all search results for blocked content not just the exact URL they are trying to reach
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		We don't have a documented Filtering Policy, however all filtering information is available through the website - https://exa.net.uk/contentfiltering-surfprotect/
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		As standard all sites are set up the same, where changes are required the customer can request these and they can be deployed to all sites.
• Identification - the filtering system should have the ability to identify users		As long as the customers are using a method of filtering
		which is possible for us to identify users then we can

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). Providers should be clear about the capacity of their filtering system to manage content on mobile and web apps		Exa filter content at a network level rather than device, filtering is done on app, mobile, browser etc.
Multiple language support – the ability for the system to manage relevant languages		The blocklist is multilingual the organisation will soon publish the list of languages we block.
Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)		All filtering is applied at network level
Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school		Quantum+ service using VPN or captive portal applies filtering on remote devices
Reporting mechanism – the ability to report inappropriate content for access or blocking		Customers can send tickets into Exa or can change their own filtering settings
Reports – the system offers clear historical information on the websites users have accessed or attempted to access		Activity logs are generated and customers can access their own logs
Safe Search – the ability to enforce 'safe search' when using search engines		If the search engine provides safe search we have the ability to enforce it

Filter Test Results for St Peter's CofE Junior School

Tests were performed at 14/09/2023 14:30

Your Connection

Type

Schools

IP Address

82.219.17.10

Reputation

Good

Organisation

St Peter's CofE Junior School

Postcode

NG11 6GB

Filtering Provider

Exa Networks

Network

EXA-NETWORKS Exa Networks Limited

Results Overview

✓

Child Sexual Abuse Content

✓

Terrorism Content

✓

Adult Content

✓

Offensive Language

Child Sexual Abuse Content

 Blocked	Description	Results & Recommendations
	Tests whether you are blocking websites on the IWF Child Abuse Content URL list.	It appears that your filtering solution includes the IWF URL Filter list, blocking access to Child Sexual Abuse content online

Terrorism Content

 Blocked	Description	Results & Recommendations
	Tests whether you are blocking websites on the Counter-Terrorism Internet Referral Unit list (CTIRU).	It appears that your filtering solution includes the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online

Adult Content

 Blocked	Description	Results & Recommendations
	Test whether your Internet filter blocks access to pornography websites	It appears that your filtering solution includes blocking for online pornography

Offensive Language

 Blocked	Description	Results & Recommendations
	Accesses a page containing offensive language to test if your filtering software blocks it	It appears that your filtering solution includes blocking for offensive language

Filter Test History for 82.219.17.10

