Filtering & Monitoring

SurfProtect®

We designed and built our content filtering platform, SurfProtect® Quantum, to fulfil Keeping Children Safe in Education (KCSiE) and The Prevent Duty guidelines in the most cost-effective way. SurfProtect Quantum is a cloud-based, fully customisable service that provides effective safeguarding measures, whatever your needs.

Quantum+ Overview

SurfProtect®

We designed and built our content filtering platform, SurfProtect® Quantum, to fulfil Keeping Children Safe in Education (KCSiE) and The Prevent Duty guidelines in the most cost-effective way. SurfProtect Quantum is a cloud-based, fully customisable service that provides effective safeguarding measures, whatever your needs.

SurfProtect® Quantum

Since 2004, we've been providing schools around the country with high-quality content filtering via our SurfProtect service. With many classes moving online, and staff working from home during the pandemic, filtering requirements have changed. To meet this need, we've developed SurfProtect Quantum+.

Quantum+

Quantum+ provides more advanced features for those who need them, including SurfProtect Anywhere which bridges the gap when it comes to filtering school devices when in use at home.

Further features include Captive Portal which allows log in to user profiling and reporting on BYOD devices, Google SSO and Azure AD integration and a higher throughput of up to 1Gbps. Quantum+ has been designed to work with any Operating System and web browser (browsers under 5 years old)

Both SurfProtect products work in conjunction with Securus' monitoring software to provide a comprehensive solution to suit your requirements.

SurfProtect® Product Comparison:

Features	Quantum	Quantum+
Active Directory integration	✓	✓
Categorisation and filtering of HTTPS and HTTP sites	✓	✓
Search and social filtering	✓	✓
Network Level BYOD	✓	✓
Analytics, reporting and real-time alerts	✓	✓
Speed throughput of 330Mbps (As standard)	✓	
Speed throughput of 1Gbps (As standard)		✓
One year's worth of reports and logs		✓
Captive Portal - filters BYOD devices with per user profiling and reporting		✓
Google SSO and Azure AD integration		✓
SurfProtect® Anywhere - filter devices even when at home		✓
Meets the requirements of DfE KCSiE, Prevent Duty and Ofsted	✓	✓

Exa Networks, 100 Bolton Road, Bradford, BD1 4DE
Registered Company Number: 04922037
Exa is a Trading Name of Exa Networks Limited

exa.net.uk 0345 145 1234 info@exa.net.uk


exa education
Internet & Filtering for Schools
Keeping children safe in education: Online safety and SurfProtect® Quantum
SurfProtect
since 2004

"Completely re-written in 2016 to reflect the ever-changing Internet world"

On September 5th 2016, the new guidelines issued by the Department for Education for 'Keeping Children Safe in Education' came into effect.

One key part of these revised statutory guidelines is online safety (Annex 3, pages 61-62), which details how governing bodies and proprietors must "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 college's IT system."

In response to these guidelines, the UK Safer Internet Centre has published helpful guidance as to what an "appropriate" monitoring policy might look like for schools. This is available to view at: www.exa.is/appropriate.

This guide explains how SurfProtect Quantum can help your school to meet these guidelines, and implement the most effective & appropriate filtering policy possible - ensuring that both staff and students are protected from the dangers present online.

If you have any queries about SurfProtect Quantum, or its compliance with the DfE guidelines, please don't hesitate to get in touch with our team on education@exa.net.uk or 0345 145 1234.

You can also learn more at www.surfprotect.co.uk.

1) Filtering Content

SurfProtect Quantum automatically implements a default filtering policy which prevents access to the most commonly-blocked web categories. This provides you with an instant degree of protection which covers the types of content and communication detailed below, as advised by the UK Safer Centre as being the minimum restrictions a school should enact.

However, it is also incredibly easy to build on this profile to create a bespoke filtering policy that is perfect for your school. SurfProtect Quantum's categorised filtering feature means that you can restrict inappropriate material in a matter of minutes – simply click on the types of websites you'd like to prevent access to and they'll be blocked immediately.

And, because many websites now host more than one type of content, it is important that they can be correctly identified as belonging to multiple categories. SurfProtect Quantum is able to assign multiple classifications per site, so you have finer control on what is viewable and what is blocked.

Content	Definition	Blocked by SurfProtect by default?
Illegal	The content displayed is illegal and therefore not allowed to be viewed by law e.g. child abuse images, terrorist material.	Yes. The category 'Criminal Activity' is blocked by default so illegal content cannot be viewed.
Bullying	Content or communication which involves the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others.	Websites which contain violent or aggressive content are automatically restricted by default.
Child Sexual Exploitation	Communication which encourages the child into a coercive/manipulative sexual relationship. This may include encouragement to meet.	The IWF's CAIC list is automatically incorporated into SurfProtect, along with all other child abuse content, to ensure that these websites are instantly blocked.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity.	Yes. Our 'Intolerance & Hate' category includes all content relating to discrimination.
Drugs/substance abuse	Displays or promotes the illegal use of drugs or substances.	Yes. SurfProtect's 'Illegal Drugs' category is blocked by default.
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance.	Yes. The category 'Intolerance & Hate' restricts radical content.
Pornography	Displays content of sexual acts or explicit images.	Yes. SurfProtect's 'Adult/Sexually Explicit' category is automatically restricted.
Self Harm	Promotes or displays deliberate self harm being performed.	Yes, content relating to self harm is blocked under the 'Suicide' category.
Violence	Displays or promotes the use of physical force intended to hurt or kill.	Yes. The categories 'Violence' and 'Weapons' are actively blocked.
Suicide	Content or communication which promotes or encourages committing suicide; or suggests that the user is considering ending their life.	Yes. The suicide category is automatically restricted by SurfProtect's default setting.

2) The Prevent Duty

In July 2015, the government placed a statutory duty on schools to ensure that children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering.

SurfProtect Quantum helps you to ensure that your school is in compliance with the Prevent duty. In our panel, you'll find a range of 'Umbrella Behaviour' settings which immediately block certain categories – one click of the 'Prevent' button will automatically block all sites which could contain radical content. This includes the categories Weapons, Violence, Intolerance & Hate, and Criminal Activity.

The Prevent setting will also enforce a block on search terms relating to extremism; this keyword list includes all terms identified by the DfE as being commonly used in ISIL dialogue and propaganda, so your students are unable to use these words to search for related material.

Using an Umbrella setting provides you with the additional security that any changes made to your school's filtering policy which could compromise your compliance with the Prevent regulations are unable to take effect unless the 'Prevent' category is specifically made inactive. This is because it locks down the relevant settings so that they cannot be overridden by any other subsequent amendments – helping to make sure that you don't accidentally compromise your compliance with this aspect of the duty.

The Counter Terrorism Internet Referral Unit list (CTIRU) is also fully integrated into SurfProtect Quantum to prevent unlawful terrorist content being veiwed.

3) Monitoring Content

Alongside enacting an effective filtering policy, it is also important for schools to implement a monitorng system to ensure that they have visibility over the website access and search term usage of individuals.

As SurfProtect Quantum enacts Active Directory integration, its Analytics feature enables you to see which user has requested banned content – either by entering a restricted search term, or attempting to view a blocked website. This means that you have complete traceability over all online activity.

With SurfProtect Analytics, you are also able to download reports of all online activity performed on your network, giving you a detailed insight into your school's web traffic over an extended period of time. Compiling and storing this data over three month periods, you can be assured that you have access to every website visited and every search term entered over this time so, should an e-safety incident occur, you have a physical record to reference.

4) Age Appropriate Filtering

Although it is incredibly important to ensure that students are unable to access offensive or dangerous material online, the guidelines also make clear that schools need to "be careful that "overblocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding." Simply enforcing a blanket ban on all potentially inappropriate material can leave both students and teachers unable to access key resources – and also make it difficult to educate pupils on responsible internet use as they progress through school.

With SurfProtect Quantum, you can allow different year groups varied levels of access. Using the per-computer filtering feature, you can create specific profiles which are appropriate for pupils' age – for example, very young students might benefit from a walled garden setting in which only certain websites are viewable and all others are blocked, whilst older pupils may require a more liberal approach.

With SurfProtect Quantum's Active Directory integration feature, you can create even more user-specific profiles – making it possible to create separate policies for groups, subject classes, and even individual users. And, using the profile prioritisation feature, you can ensure that students always receive the most appropriate level of filtering for their age.

5) BYOD Filtering

The DfE guidelines also highlight the issue that "many children have unlimited and unrestricted access to the internet via 3G and 4G" and that a clear policy on the use of mobile technology is therefore required. This is particularly important for those schools implementing a BYOD (Bring Your Own Device) scheme where the tablet will be used in the classroom, or for educational purposes.

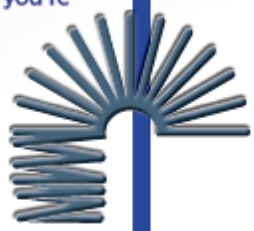
With SurfProtect Quantum, it is possible to ensure that every device – whether static or mobile, owned by the school or the student – receives the same level of protection. This is because SurfProtect Quantum implements network-level filtering, which means that all traffic on the school's internet connection is filtered – regardless of the machine or device used to access it.

However, if the student is using their own data on their own device, it is not technically possible to implement a filtering policy on this internet usage as the student will not be touching the school's internet connectivity – and therefore SurfProtect Quantum – at all. In this situation, a clear e-safety policy is incredibly important as it enables the school to teach students about what is and is not appropriate to be viewed, both in and out of the education environment.

6) Flexible Filtering

We understand that content filtering isn't a one-size-fits-all matter. That is why SurfProtect Quantum's filtering policies are completely customisable, so that you can implement the exact level of filtering you want for your school – and the intuitive, user-friendly design makes it easier than ever before to change your settings as and when you need to.

SurfProtect Quantum's web-based portal means that authorised staff members can review and edit filtering policies any time they're connected to thenternet – giving you total convenience, and making sure that you're always in control of your content filtering. And, SurfProtect Quantum provides you with the ability to allow or block specific websites – regardless of their category classification – so you can be assured that you will always be able to implement the filtering setting you need for your school. With all updates taking place in real time, you will never have to wait around for key resources to be unlocked, or inappropriate material to be restricted.



7) Search Term Filtering

Blocking search terms can be an invaluable tool in preventing students from viewing dangerous material online. By restricting the ability to search for offensive content, pupils are immediately aware that their request is inappropriate – and are also unable to see any related material.

SurfProtect Quantum's categorised 'Restricted Search Terms' feature means that you can apply specific groups of search terms, whilst not enforcing others. For example, you may wish to prevent pupils searching for terms relating to extremism, but allow them to search for games. SurfProtect Quantum enables you to implement the perfect settings for your school in a matter of moments.

We frequently update our lists of restricted terms to ensure that they are as effective and relevant as possible. However, you also have the ability to add your own terms, or remove ones you don't feel to be appropriate for your school's e-safety policy. For example, you may wish to allow students – particularly those in higher year groups – to search for 'Mein Kampf' or 'Reich', but still enforce the 'Extremism' category as a whole. With just a few clicks, you can allow the searches you require whilst still ensuring that pupils are protected from viewing radical material.

We have also introduced an additional layer of protection by applying the 'Restricted Search Terms' feature to YouTube searches – helping to prevent pupils from requesting offensive videos.

Safeguarding Support

The content filtering and monitoring tools employed by a school form an integral part of their online safeguarding, however, the DfE also states that they should "consider how children may be taught about safeguarding online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum."

Created in October 2015, exa.foundation is part of Exa Education, and is dedicated to providing schools with the advice, resources and guidance needed to embrace everything technology has to offer – safely.

That is why we provide an e-safety course focusing on keeping students safe and secure online, covering topics on everything from grooming, cyber bullying and digital footprints to phishing, gambling and CEOP. And, if you're an Exa Education customer, you receive access to this – and all other exa.foundation services – completely free of charge.

Alongside individual events for schools, we also organise national exa.foundation conferences, provide online courses and much more...

If you would like to learn a little more about exa.foundation, or to organise a course or event to take place at your school, please don't hesitate to get in touch with a member of our team.

0345 145 1234
info@exa.foundation
www.exa.foundation

exa
.foundation

SurfProtect.co.uk | exa.education | 0345 145 1234

SurfProtect Prevent Duty

exa education
Internet & Filtering for Schools

The Prevent Duty

In July 2015, the government placed a statutory duty on schools to keep children safe from the risk of radicalisation and extremism. This expectation made clear that every teacher must be aware of the risks posed by the online activity of extremist groups, and how social media is being used to encourage young people to travel to Syria and Iraq.

How can SurfProtect® Quantum help?

SurfProtect Quantum helps you to ensure that your school is in compliance with the Prevent duty through the following features:

- **One-Click Compliance.** In our panel, you'll find a range of 'Umbrella Behaviour' settings which immediately block certain categories – one click of the 'Prevent' button will automatically block all sites which could contain radical content. The Prevent setting will also enforce a block on search terms relating to extremism; this keyword list includes all terms identified by the DfE as being commonly used in ISIL dialogue, so students are unable to use these words to search for related material.
- **Social Media.** As radical conversation and activity takes place on a variety of social media platforms – rather than designated websites – you may also opt to restrict access to this category, and sites such as YouTube which have prolific comment sections that may be abused. SurfProtect's flexibility ensures that it is possible for a school to still allow access to the web pages, videos, or channels within these blocked categories & websites which have an educational purpose.
- **User Reporting.** SurfProtect Quantum provides you with a detailed insight into the activity taking place on your school's internet connection – from which sites are being requested, which are most frequently visited and even which students are attempting to access which sites. As a result, you are able to identify any causes for concern, and possible intervention.
- **Home Office Terrorism Watch List.** The CTIRU (Counter Terrorism Internet Referral Unit) list is fully integrated into SurfProtect Quantum. This means that all sites and search terms identified by the CTIRU as being related to terrorism are blocked by default and cannot be accessed. This list cannot be removed or amended by either staff or students, so you can be assured you are always compliant with this aspect of the Prevent duty.
- **Peer to Peer.** We work tirelessly to ensure that peer to peer sites, such as Tor, are correctly categorised. This means that once a School has blocked this category, it is incredibly difficult for students to download these applications which are commonly used for sharing offensive and inflammatory content.
- **News & Politics.** It is also possible to block more wide-reaching and general categories, such as News, Politics and Religion, which will include a great deal of informative material but which may also include some, or reference to, extremist content.

To learn more, please don't hesitate to get in touch on **0345 145 1234** or **education@exa.net.uk**

SurfProtect
since 2004


exa education
Internet & Filtering for Schools
SurfProtect
since 2004
SurfProtect®
Quantum
FAQs

SurfProtect Quantum

Our brand new content filtering service offers an incredible number of benefits to the way in which a school is able to protect both staff and students in today's digital world.

Providing categorised, age-appropriate filtering, BYOD protection, search term filtering, safeguarding support, subscription to the IWF and Home Office Terrorism Watch List, and the flexibility to create the exact level of filtering you want for your schools, you can be assured that SurfProtect Quantum protects both staff and students from the many dangers present online – and that they are in accordance with the current DfE framework.

How does it work?

Located entirely in the cloud, SurfProtect Quantum performs network-level filtering. This means that all traffic on a school's internet connection is filtered, regardless of the machine or device used to access it. The simple installation of an AD proxy enables AD integration to be performed, so you can receive individual user filtering and reporting. As a result, you do not need to install any hardware on your schools' premises – instead, you can be assured that they are receiving industry-leading protection, without having to configure and maintain an on-site device!

When will it be available to buy?

Currently in early release, SurfProtect Quantum is available to buy now.

Offering the functionalities previously only available with SurfProtect Fusion, SurfProtect Quantum will bring individual user filtering, complete HTTPS protection and reporting features to every customer. If your schools are using SurfProtect Fusion at the moment, they will still receive the advanced online analytics provided with SurfProtect Quantum without transitioning to the service – and we will continue to support existing Stormshield devices for as long as our customers require us to do so. However, if on renewal of hardware maintenance, a school would like to migrate to SurfProtect Quantum, we would be more than happy to arrange this for them.

For those schools using SurfProtect Cloud or Proxy, they are able to transition to SurfProtect Quantum at a time that is most convenient for them. In moving to Quantum, they will become compliant with the DfE guidelines which require all websites accessed or requested on a school's internet connection to be logged, and will also receive AD integration and complete HTTPS filtering. It is important to note that SurfProtect Quantum has been built in line with the Internet standards, however, we have and still are encountering some products and applications which do not conform to these standards and we are therefore creating workable solutions in these situations.

How much does it cost?

Until the end of this year, SurfProtect Quantum is free for you and all your schools to order – and you will not begin paying for the service until their annual renewal occurs in 2018. After this time, for Exa Education connectivity customers, it will cost just £100 for primaries and £250 for secondaries. If a school uses an alternative ISP for their connectivity, SurfProtect Quantum is available for £1,000 – subject to availability.

If you have any questions or concerns regarding SurfProtect Quantum, please get in touch with your account manager, call the team on **0345 145 1234** or send an email to **education@exa.net.uk**

Key Features

Cloud Filtering

As SurfProtect Quantum 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 Quantum 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 Quantum 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 Quantum 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 Quantum, 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.

SurfProtect
since 2004

SurfProtect.co.uk | exa.education | 0345 145 1234

SurfProtect Quantum Setup Guide

SurfProtect® Quantum Setup Guide

Located entirely in the cloud, SurfProtect Quantum performs network-level filtering. This means that all traffic on your school's internet connection is filtered, regardless of the machine or device used to access it. As a result, you do not need to install any hardware on your school's premises* - instead, you can be assured that you are receiving industry-leading protection, without having to configure and maintain an on-site device!

Providing categorised, age-appropriate filtering, BYOD protection, search term filtering, safeguarding support, subscription to the IWF and Home Office Terrorism Watch List, all with the flexibility to create the exact level of filtering you want for your school, you can be assured that SurfProtect Quantum protects your staff and students from the many dangers present online - and that you are in accordance with the current framework.

Below we have detailed many of the features you will receive with SurfProtect Quantum.

Filtering	
HTTP filtering	✔
HTTPS decryption	✔
Intercept BYOD	✔
Realtime classification	✔

Encrypted Websites	
Enforce Google SafeSearch	✔
Keyword filtering	✔
Restricted YouTube	✔

Identification	
External IP	✔
Username	✔
Groups	✔
Full IPv6 support	✔

Single Sign-on	
Active Directory	✔

Logs	
Downloadable logs of all filtered traffic	✔
Includes all search queries	✔
Indicate user	✔

Analytics	
Analytics dashboard	✔
Search query report	✔

Administration	
Centralised control panel	✔
Single sign-on authentication	✔

In order to receive completely cloud-based filtering, there are a few things to do on your network which enable us to perform AD integration and HTTPS filtering on your school's internet connection.

Please complete the following steps to allow these features of your filtering service to be enacted. If you require help at any point, please do not hesitate to contact our dedicated support team on **0345 145 1234** or by emailing **support@exa.net.uk**.

exa education

*If you are an external SurfProtect Quantum customer and do not wish to deploy the proxy to each device, you will require a firewall as this enables us to implement DNAT rules to force your internet connection to SurfProtect Quantum for filtering to be performed.

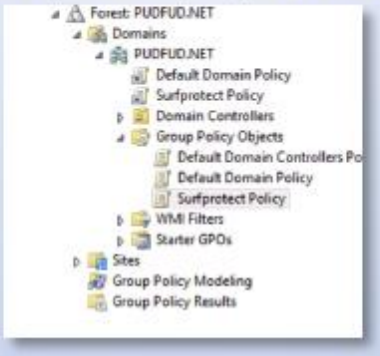
SurfProtect Quantum Certificate Setup

SurfProtect's cloud-based HTTPS filtering feature requires that all devices on your network trust Exa Education. This document provides guidance to enable this across your network, however, should you require any additional help then please do not hesitate to contact our dedicated support team on 0345 145 1234 or by emailing helpdesk@exa.net.uk

A certificate published by Exa Education needs to be installed on each device within your network. This can be done on a per machine basis, however we have detailed how to deploy the necessary certificate using various management tools below.

Deployment with Active Directory

1. Download your SurfProtect Quantum certificate at www.exa.is/certificate
2. Once you are logged into your active directory server, go to Start > Administrative Tools > Group Policy Management
3. Identify the Group Policy Object that you wish to edit (optionally, you may wish to create a new Group Policy Object to define all surfprotect settings in one place)
4. Right click the newly created Group Policy Object and select edit
5. Navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies
6. Right click on the folder Trusted Root Certification Authorities and select Import
7. Follow the steps in the Certificate Import Wizard, providing the location of the certificate downloaded from the SurfProtect panel when prompted for a file to import.



exa education

Version 2.0

Deployment with Google Admin Console (GSuite)

1. Download your SurfProtect Quantum certificate at www.exa.is/certificate
2. Log into the admin panel at https://admin.google.com
3. Navigate to Device Management
4. In the DEVICE SETTINGS menu on the left, select Network
5. Select Certificate > ADD CERTIFICATE
6. Navigate to the previously downloaded certificate
7. Ensure that the option labelled Use this certificate as an HTTPS certificate authority is checked
8. Click Save

Individual Windows Machine Installation

1. Download your SurfProtect Quantum certificate at www.exa.is/certificate
2. Click the Windows Start Button and type '*mmc*' into the search bar to locate and run the Microsoft Management Console
3. Navigate to the File menu > Add/Remove Snap-in
4. From the Available snap-ins pane, select Certificates and then click on the button labelled Add
5. In the Certificates snap-in wizard, select computer account or local computer when prompted for which context the snap-in should manage certificate for.
6. Click Finish to close the wizard and OK to close the snap-ins window
7. In the console tree, double-click on Certificates
8. Right-click the Trusted Root Certification Authorities and click import
9. Follow the steps in the Certificate Import Wizard, providing the location of the certificate downloaded from the SurfProtect panel when prompted for a file to import

Individual Mac OS X Installation

1. Download your SurfProtect Quantum certificate at www.exa.is/certificate
2. Launch Keychain Access
3. From the Keychain Access toolbar, select File > Import Items
4. Provide the location of the downloaded certificate when prompted for a file location and click Open
5. Double-click on the newly imported certificate, labelled Exa Networks Ltd CA
6. In the Trust section of the newly opened window, set the value in the dropdown labelled Secure Sockets Layer (SSL) to Always Trust
7. Close the current window to apply changes
8. Enter your system password when prompted and click on Update Settings

exa education

Version 2.0

Individual Chromebook Installation

1. Download your SurfProtect Quantum certificate at www.exa.is/certificate
2. Scroll to the bottom of your Chromebook's Settings page and click on Show advanced settings
3. Under the HTTPS/SSL section, click on Manage certificates
4. Navigate to the Authorities tab in the Certificate Manager and click Import
5. Select the certificate from your Downloads location and click on Open

Individual iOS Installation

1. Navigate to exa.is/certificate
2. Tap Allow on the pop-up

3. On the following screen tap Install (if using iOS 12.x, you can find this in Settings > Profile Downloaded)

4. Input your Passcode if prompted
5. Confirm by tapping Install
6. Return to Settings and follow: General > About > Certificate Trust Settings and Enable 'Exa Networks Ltd Root CA' by tapping the slider.

Individual Android Version 7 Installation

1. Navigate to www.exa.is/certificate
2. This will prompt a download, click open
3. Input your Passcode when prompted
4. Set the Certificate name then choose credential use as VPN and Apps option.
5. Tap OK, this will then install and become a user certificate.

exa education

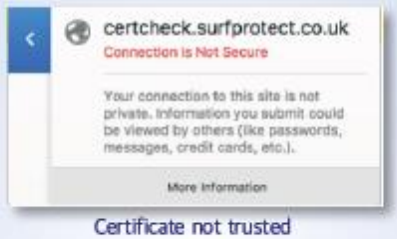
Version 2.0

Installation Verification

You can check whether the certificate is being successfully trusted by visiting the SurfProtect Certificate Status page at http://certcheck.surfprotect.co.uk

This page will automatically detect the location you're browsing from so it can present a certificate signed by the authority you've trusted during negotiation of the secure HTTPS connection. If your browser shows that the connection is safe then this validation serves as proof that the service certificate is trusted.

Certificate successfully trusted



Certificate not trusted

If you don't already have SurfProtect configured to transparently decrypt all web traffic you can test decryption by configuring your browser to use proxy.quantum.exa-networks.co.uk on port 3128.

exa education

Version 2.0

SurfProtect Quantum AD Configuration

SurfProtect Quantum integrates with Active Directory to provide 'per user' policy filtering and reporting. To achieve this, your AD data needs to be imported to SurfProtect. This document provides guidance on this process, however, should you require any additional help then please do not hesitate to contact our dedicated Technical Support team on 0345 145 1234 or by emailing support@exa.net.uk

IMPORTANT: If you do not want to enact the AD integration feature of SurfProtect Quantum, or do not have an AD server, you do not need to perform the following steps.

This will prevent these devices accessing any website belonging to a restricted SurfProtect category, or any website that you have added to your blocked list.

Why synchronise your Active Directory data with SurfProtect?

Individual users are represented in Active Directory by a unique user account and by membership to an arbitrary number of group accounts.

With Active Directory integration enabled, SurfProtect can apply different filtering policies to unique users as well as group accounts.

SurfProtect also uses the information from the data synchronisation to display the real names of your users to enrich the data provided by our data analytics panel.

Steps

1. Download the SurfProtect Quantum configuration script at www.exa.is/installing
2. Right click on the downloaded file and select 'Run with Powershell'
   NOTE: This script must be run directly on your Active Directory domain server in order to perform all necessary configuration.
3. Select 'Open' in the security dialogue box that appears.
4. Follow the commands on screen, the script should complete in a matter of minutes.
5. Please call our Technical Support team on **0345 145 1234** once these steps have been performed.

exa education

Version 1.3

Single Sign-On

Single sign-on (also known as SSO) is an authentication service that allows a user to access multiple applications with one set of login credentials (e.g. username and password), often without the need to retype these details once they have logged in to the computer.

Why is SSO important for SurfProtect?

SurfProtect communicates with popular SSO schemes in order to obtain information about which user is accessing a web page or other resource hosted on a website. This information is used both to provide granular filtering control, and to ensure that the logs and reports available with SurfProtect Analytics clearly identify which user accessed or requested which online content.

Windows Active Directory

SSO is achieved with Active Directory by requesting a user's information from the web browser whenever a web resource is requested by a machine in your school's local domain.

Running the above script will establish trust between your school's domain controller and our proxy servers. This means that when a user requests access to a website, the web browser will be able to communicate with the domain controller to identify the individual and provide SurfProtect with trusted proof of who that person is. As a result, SurfProtect can then filter the web request according to that individual's filtering profile, and record their online activity.

As SSO requires direct authentication against our proxy servers, Active Directory SSO requires web browsers to be configured with explicit proxy settings. Fortunately, these settings can be pushed to all Windows devices by creating a Group Policy Object; using this mechanism also helps to prevent settings from being manually changed by students.

Mixed Environments

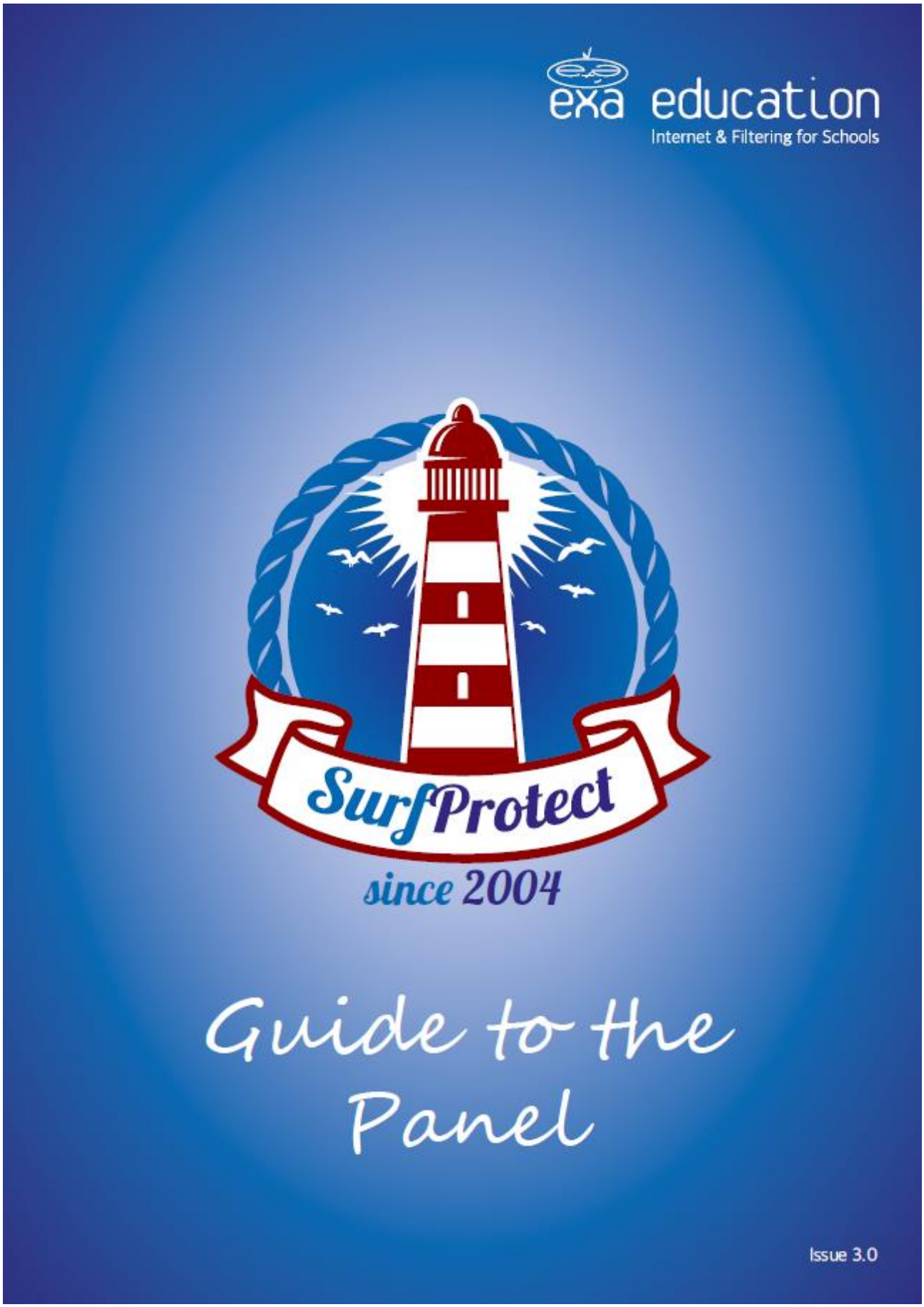
If your school uses devices outside of your AD domain, such as iPads and Chromebooks, which are not managed as part of your local domain, individual user filtering and identification will not be possible.

These devices will still receive transparent SurfProtect filtering when connected to your school's network, however user identity information and profile matching will not be enacted and web logs will not be populated with user or machine identities.

Depending on your school's mobile device and guest internet policies, it may be that you wish to always prevent unlogged internet access from being performed. If this is the case, you can disable non-authenticated filtering in the SurfProtect panel. In doing this, students or visitors attempting to access the school's internet service on a mobile device will be presented with a screen which advises that they are unable to do so and must instead login to a configured machine.

exa education

SurfProtect Quantum Guide to Panel



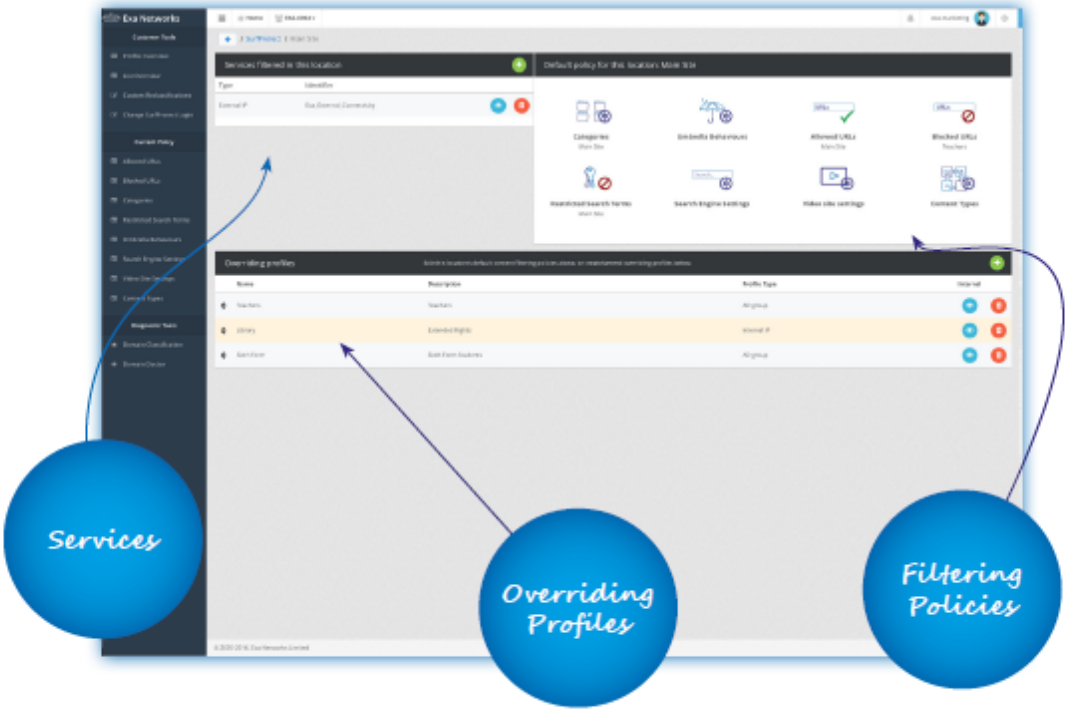
The SurfProtect Panel Guide.

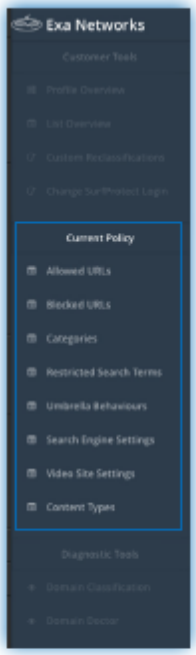
Welcome to the all-new SurfProtect - even if you are a veteran SurfProtect user, you will still benefit from familiarising yourself with the new interface with the help of this guide.

As always, if you require help with any aspect of your content filtering solution, please do not hesitate to get in touch.

Log in!

Visit panel.surfprotect.co.uk to log in, your credentials have not changed, once you are qualified through security you will see your all-new home page which for most users, is the main screen that shows you the filtering policies that are applied to your network. Let's take a deeper look...





General Navigation

There are three main sections on your home page which are identified above.

Services shows which Internet connections are covered by your filtering policies

Filtering Policies is where you control all the active policies of your filtering

Overriding Profiles lists any users or groups of users which are treated differently to the default policies set in 'Filtering Policies'

From the left hand navigation panel you can access shortcuts to each of the policy sections.

You can also access general Customer and Diagnostic Tools from this menu. (See pages 13 - 15).

Locations

A location is defined as a physical site. For the majority of schools there will just be one location which is the school. However, some schools may wish to define a separate location for other sites such as remote campuses or boarding dormitories. Filtering policies are per location.

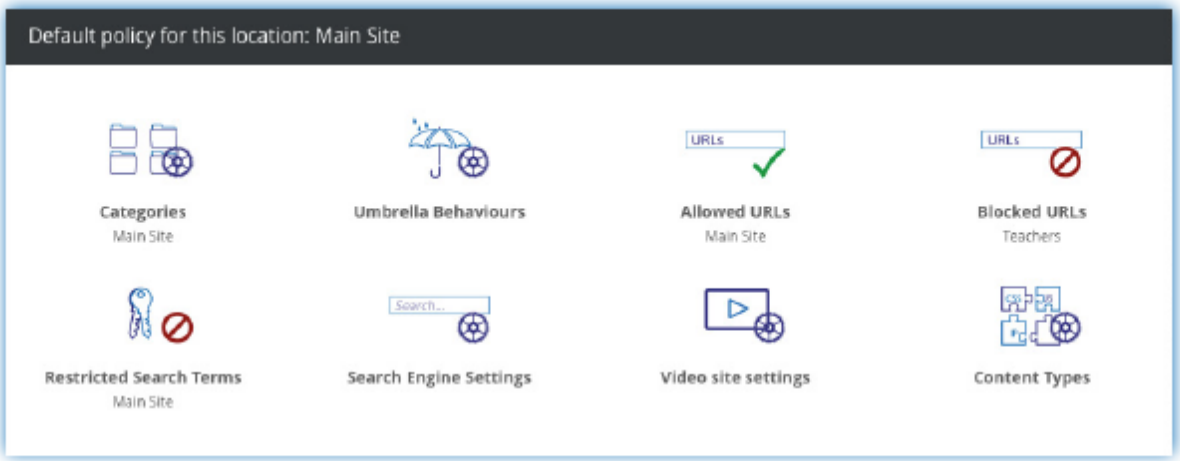
Connections in this location

Here we can see which of your Internet connections are covered by this location. For many of our customers this will be just the one connection, however, if you have more than one connection (e.g. a back-up or an additional connection they can be added easily by clicking

Default policies for this location

This is the hub of all filtering policies.

Building a comprehensive yet flexible content filtering package can seem like a big task, to make it easier to customise we have broken it down into manageable sections.



The title bar informs you that we are in the Location Main Site. The sections available are:

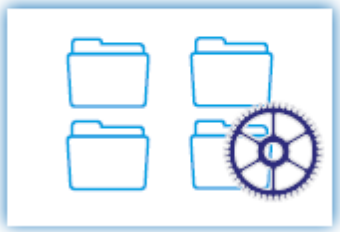
- **Categories** - Block or Allow categories of websites such as 'Adult' or 'Gambling'
- **Restricted Search Terms** - Block words from being entered into search engines
- **Umbrella Behaviours** - The ability to apply a group of settings in one click such as Prevent Duty compliance
- **Search Engine Settings** - Safe Search appliance and default search engine
- **Allowed URLs** - Explicitly permitted URLs
- **Video Site Settings** - Apply Safe Search to video sites
- **Blocked URLs** - Explicitly blocked URLs
- **Content Types** - Block or Allow elements of websites.

The sections for Categories, Restricted Search Terms, Allowed URLs and Blocked URLs group entries into Lists for easier management. At a glance you can see the applied Lists for these sections.

Clicking on each icon will let you amend the applied settings.

> *Note:*
>
> 'Lists' are independent of Locations and Profiles, meaning that if any other Location or Profile is using the same List then they will be affected by your changes also. A notification will appear in the top right hand corner if any other Location or Profile will be affected.
> If you want the List to only apply to this Location consider creating a new List and name it something relevant. See the section 'Using Lists across multiple Profiles' on page 12 for more information.

Categories



SurfProtect treats websites differently depending on how we have classified them. When a site is classified it will fall into a category such as Sports or Arts etc. A policy defining which categories are permitted or blocked on your connection is called a List.

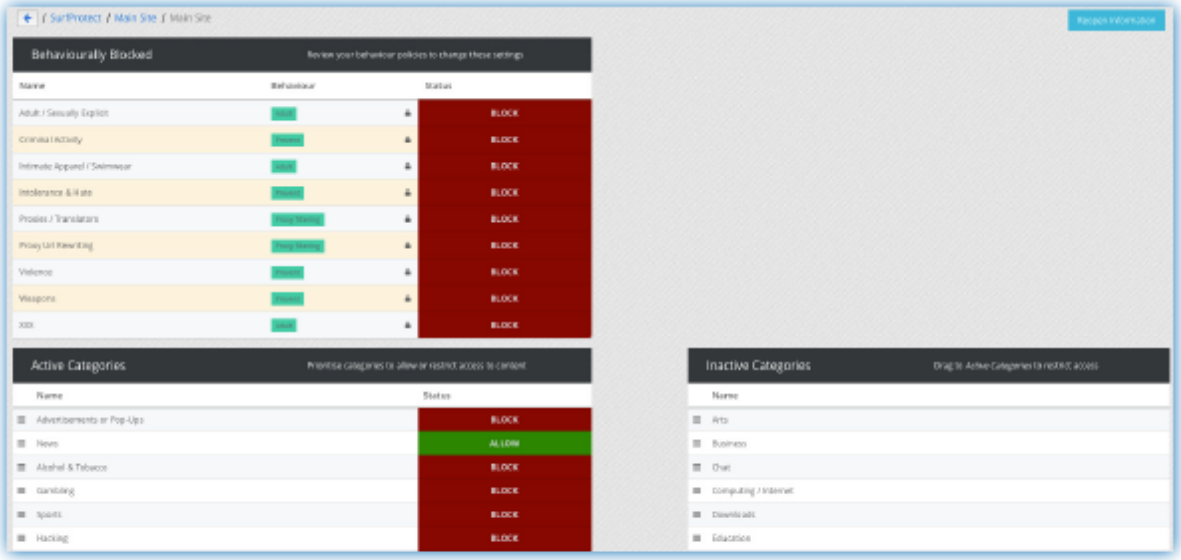
Underneath the icon you will see which category List is currently assigned. By hovering over the icon you can then choose an alternative list to apply, remove all category filtering, or, edit the current list. Let's look at editing a list; hover over the icon and choose 'Edit'.

The first thing you will see is a list of categories that are blocked by your Umbrella Behaviour settings, the middle column displays the Umbrella Behaviour that the category falls under. For your protection these cannot be unblocked here and must be done on the Umbrella Behaviour page. Click on the Behaviour to jump straight to that page.

Lower down the page shows the Active Categories and their current status. You can change the status between Block and Allow by simply clicking the status indicator. You can also add in any categories from the Inactive Categories list on the right hand side by just dragging them over.

One of the biggest changes for our new SurfProtect product is the ability to order the list, this is made possible by an all-new classification system which allows for a website to have multiple classifications and this is where the ordering comes into play:

Let's take the ESPN website as an example. This website is classified as both *Sports* and *News*. It might be that you would like News sites to be accessible on your connection, but not general Sports sites. In this scenario you would place the category News above Sports and set the status to Allow for News and Block for Sports (see below). Now, SurfProtect will allow the page to be loaded as the first classification it matches in the list is News, which is permitted. However a site which is classified as Sports, such as nba.com will continue to be blocked as Sports is the first category in the list which nba.com matches.



Restricted Search Terms

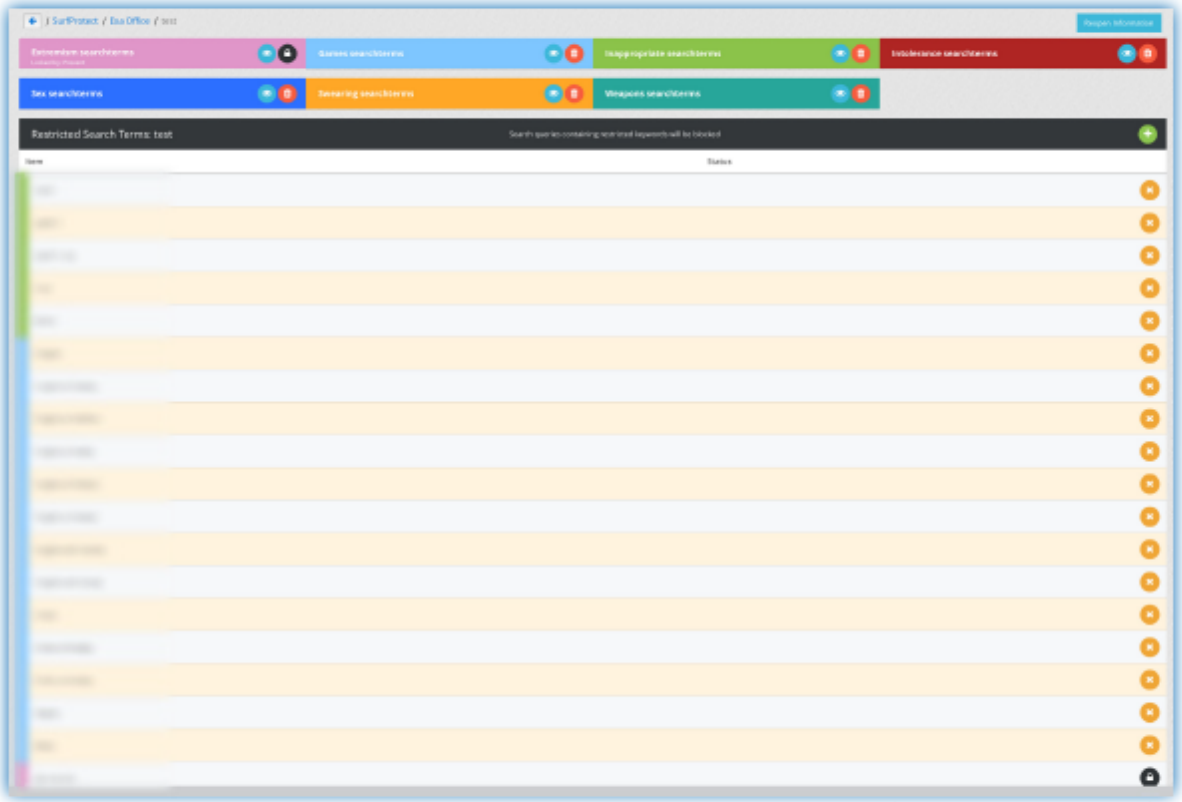
Further than the ability to block websites, SurfProtect can also affect particular parts of a site. Search Terms are indicative of this ability. Where Search Engine sites can be allowed, yet the input of inappropriate words can be blocked.

Underneath the icon you will see which Search Term List is currently assigned. By hovering over the icon you can then choose an alternative list to apply, remove all Search Term filtering, or, edit the current list. Let's look at editing a list; hover over the icon and choose 'Edit'.

On the resulting screen you are shown the pre-populated groups of keywords at the top of the page, by default these are all active. To view the keywords that are restricted by each group you can click , to opt out of that category simply click . Groups that are inherited by Umbrella Presets cannot be opted out of and will display .

Below the groups are all the resulting restricted search terms, to add your own search terms simply click . You can add a single, or multiple terms by just hitting enter after each keyword. Any user added Search Term automatically get grouped for your convenience under a 'User Added' group.

Manually added terms can be deleted from your list, however, terms that are inherited from the categories cannot be deleted but can be opted out of by clicking and will show an 'opted out' status letting you opt back in at any time. Terms belonging to Umbrella Presets will show a and cannot be opted out of.

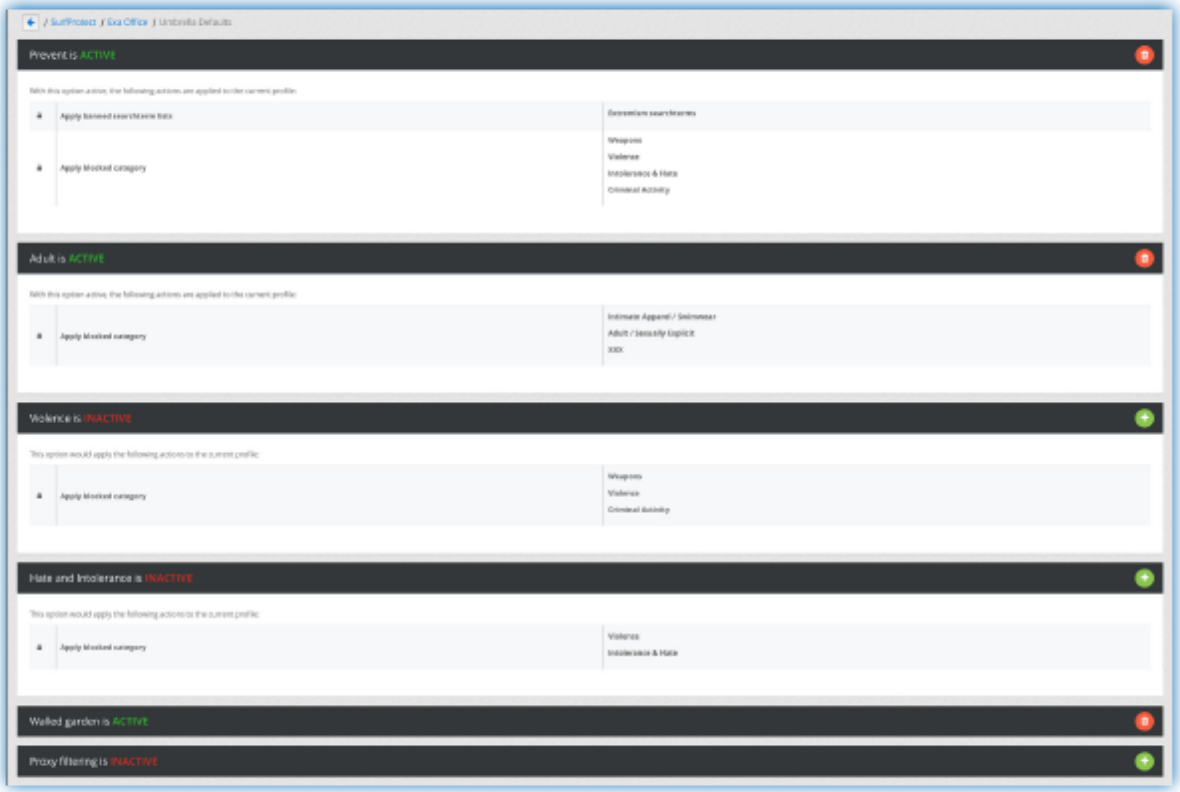


Umbrella Behaviours

A new feature of SurfProtect is the ability to apply a group of settings in one click. For example, you can apply all relevant settings for 'The Prevent Duty' by simply clicking the 'Prevent' Umbrella Behaviour.

Click the icon to select the Umbrella Behaviours that apply to your policy.

The Umbrella page shows the available behaviours and their current status. It also shows you the search term categories and website categories that are applied by each Behaviour. You can easily toggle whether a Behaviour is Active or Inactive by clicking or



Search Engine Settings

Here you can not only select your preferred Search Engine for your connection, but also decide whether to force your preferred search engine's Safe Search feature.

Hover over the icon to access the search engine menu.

Allowed URLs

There may be a time where websites that would normally be blocked by your filtering policies are legitimately required. Here you can override your other filtering policies and explicitly permit access to a web page or domain.

Underneath the icon you will see which Allowed List is currently assigned. Hovering over the icon lets you choose an alternative list, remove filtering, or, edit the current list. Let's look at editing a list; hover over the icon and choose 'Edit'.

Hit the icon to add a URL to your allowed list.
Either add the site by typing (for example) bbc.co.uk or permit the entire domain by adding a '.' before - e.g .bbc.co.uk

The search bar allows you to easily search through your allowed URL list, the search bar works in real-time and will search for strings of text as well as full words / sites.

Blocked URLs

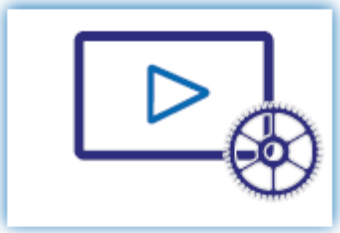
Blocked URLs work in much the same way as Allowed URLs above - you may become aware of a website that you do not want to be accessed on your connection - regardless of any filtering policies in place.

SurfProtect allows for inherited Blocked lists which are displayed at the top of this page. The shows you the sites belonging to the inherited list and the allows you to opt out. Note, the List remains there for you to opt back in at any time.

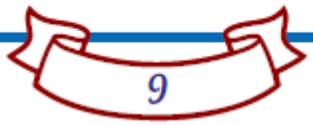
Hit the icon on to add a URL to your blocked list.
Either add the site by typing (for example) bbc.co.uk or to block the entire domain add a '.' before - e.g. .bbc.co.uk

The search bar allows you to easily search through your allowed URL list, the search bar works in real-time and will search for strings of text as well as full words / sites.

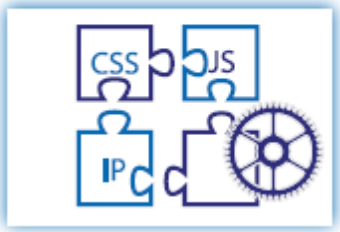
Video Site Settings



Hover over the icon to access the menu, from here you can add your YouTube ID and force Safe Search to work seamlessly with YouTube videos.



Content Types



Another new feature of SurfProtect allows you to now control elements of content from being downloaded from the Internet. Whilst this is now a possibility, we believe that the default settings are ideal for most users.

The top section refers to External Resource Compatibility and you are given the option to Always Allow:

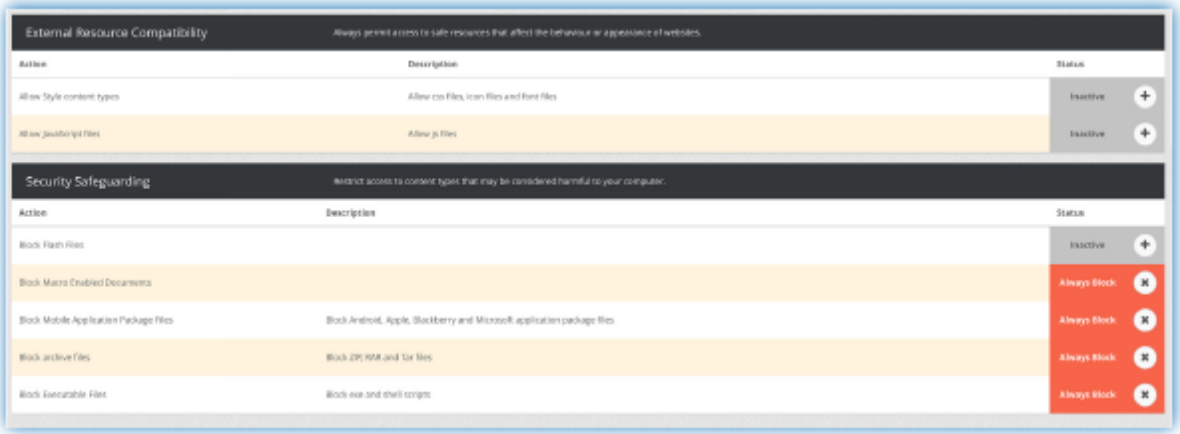
- Style content types (css, icon and font files) – These are the building blocks of websites, the default status is Inactive which means that the content will load if your other content-filtering settings permit that site from being displayed.
- JavaScript files – JavaScript is a commonly used Internet language, however can be used for malicious ends. Again, the default status is set to Inactive.

> **Note:**
>
> By changing the status of either of these you are bypassing your current content-filtering policy and explicitly allowing this type of content to be downloaded regardless of their origin.

The lower section looks after the Security Safeguarding and allows you to Always Block the following, regardless of their origin:

- Flash files
- Macro Enabled Documents – including Macro enabled Word and Excel files
- Mobile Application Package Files – Android, Apple and Blackberry applications
- Archive Files – such as Zip, RAR and Tar files
- Executable Files – .exe and shell scripts

This can be particularly helpful to defend against harmful files that are disguised as legitimate programs and files.



Your defaults are all set.

Now that we've defined your global filtering policy for all users on your connection we can start to look at any exceptions to the rule by creating Overriding Profiles...

Overriding Profiles

An Overriding Profile is an exception to your default policies. For example you may want Teachers and Students to have different filtering policies applied to them. Here we can set up a profile just to be used by teachers whilst everyone else (including students) would use the default policies we've just defined.

When you first set up your filtering policies this section will be empty. You can create an Overriding Profile for individual users or groups of users. To get started click this will launch a wizard which will guide you through the setup process.

> **Note:**
>
> The matching of users on Internal IP addresses, AD user groups or AD user names requires SurfProtect Fusion. If you are a Cloud or Proxy customer you can only create an Overriding Profile matching on External IP only.

The Wizard makes adding profiles super easy, start by giving your new profile a name and description; here we've set one up called 'Teachers'

You are then prompted on how to match the profile to your users, for our Teachers we will match them on their Active Directory group, specify the AD group name in the box provided

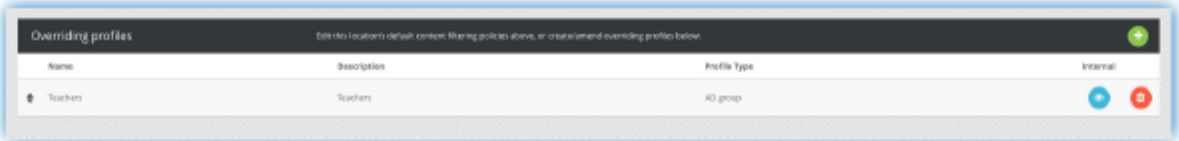
Now you can apply policies to your new group, by default, SurfProtect prompts you to create a new list for the four options available which are then configurable from within the profile, but you can use already created lists by selecting them from the drilldown boxes. Don't worry though, all this can be changed through the panel at a later time

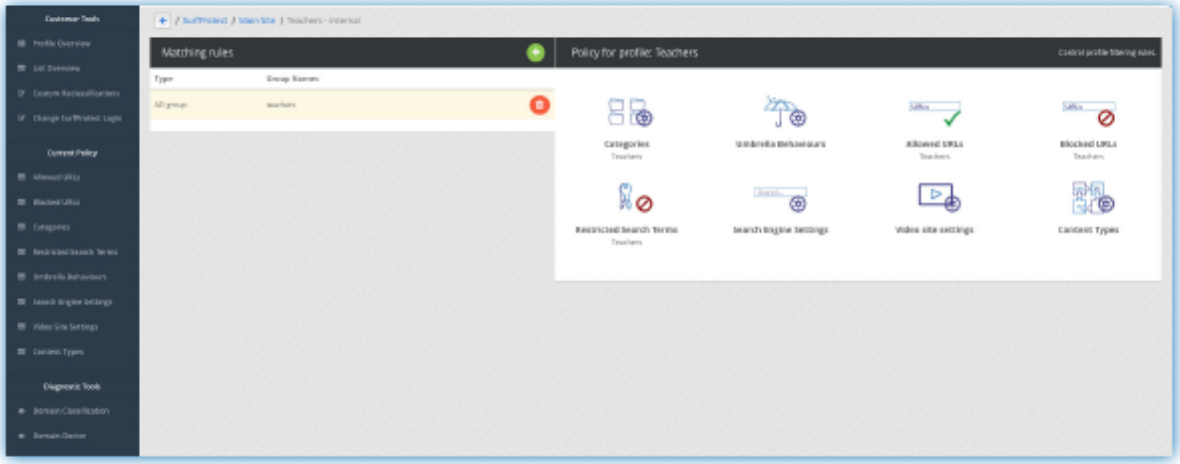
Under the Umbrella tab you can select any Umbrella behaviours you want applied to your new profile.

That's it, your new Profile is set up.

Working with Overriding Profiles

You can now see the newly created profile. Click to see the options available for your profile, this looks the same as your home page (without the Overriding Profiles section).
Clicking will remove the Profile.





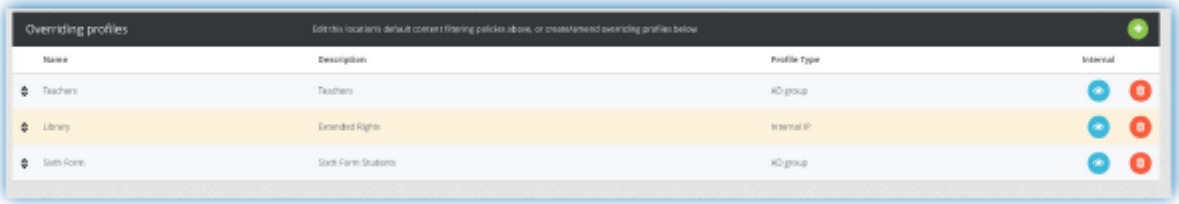
Notice how now the Categories, Restricted Search Terms and Allowed & Blocked URL lists are all set to our newly created 'Teachers' lists. This means that they will only have the default and Umbrella settings applied.

These sections act the same as they did previously when we were setting up the defaults. Now you are editing the 'Teachers' lists and any settings will only affect users matched to this profile unless you are sharing Lists (see the 'Using Lists across multiple profiles' page 12).

Using multiple Profiles

You can see below an example of a connection which uses three overriding profiles. This list is hierarchical and SurfProtect will cross-reference a users credentials against the profiles starting at the top of the list until it can match the user. In our example if a teacher was to use the Internet they would be matched against the Teachers profile and it would stop checking the rest of the list; i.e. it wouldn't matter where in the school they were. However, if a member of the sixth form was in the Library, then they would be matched as being in the library and have the Library profile applied to them as it appears higher in the list yet once they leave the library, they would then be filtered according to their Sixth Form profile.

The items can be re-ordered by dragging them up or down.



Using Lists across multiple Profiles

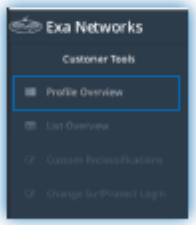
When we created a new profile, SurfProtect by default created a new list for the Categories, Restricted Search Terms and Allowed/Blocked URLs sections. However, there may be lists that can be shared, for example the Blocked URLs list may be the same for the entire school.

If the profile is set up already:
Go into the profile and hover over Blocked URLs, click PICK LIST, you can now choose from the lists already created.

If the profile is new:
During the setup Wizard, simply click the drilldown box to see lists that are already created and select the desired list.

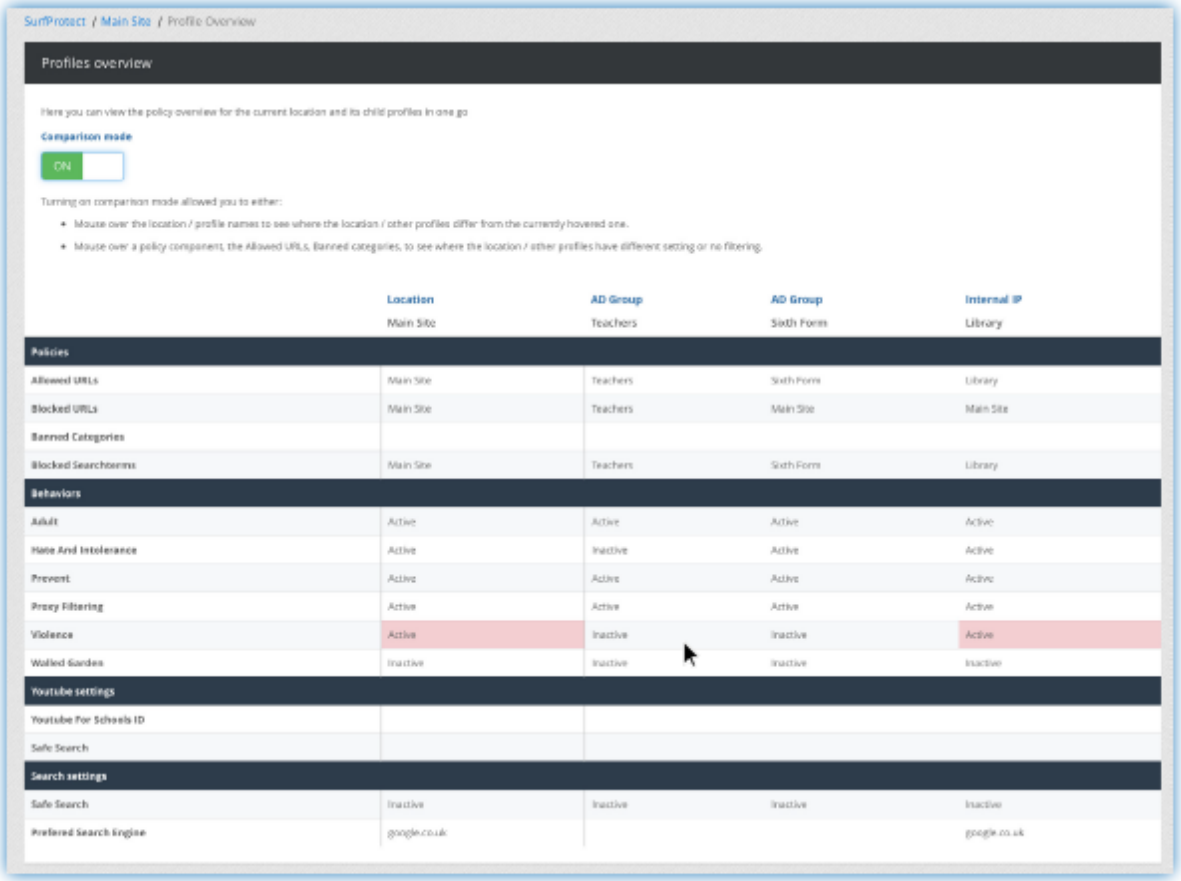
Customer Tools

Profile Overview



Located in the left hand navigation panel, the Profile Overview tool is accessible from any page. This tool directly compares your settings across multiple Locations and Profiles. In the example below you can see that our Overriding Profiles; Sixth Form & Library have separate Blocked Search Terms Lists applied, yet share the Blocked URLs List with the main site.

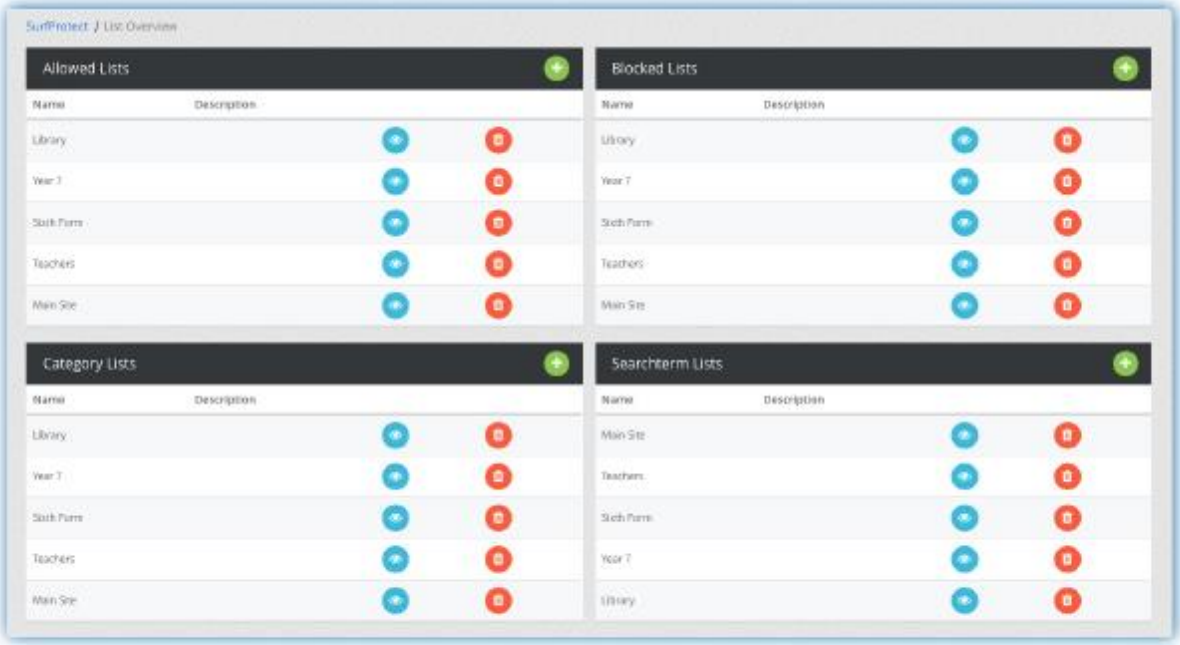
The Comparison mode aids you by highlighting differing settings.
In the image below, we have the Comparison mode active. The mouse is on the Teachers column and Violence row – showing an Inactive status. The two contrasting results (Active) are highlighted in red for you.



	Location	AD Group	AD Group	Internal IP
	Main Site	Teachers	Sixth Form	Library
Policies				
Allowed URLs	Main Site	Teachers	Sixth Form	Library
Blocked URLs	Main Site	Teachers	Main Site	Main Site
Banned Categories				
Blocked Searchterms	Main Site	Teachers	Sixth Form	Library
Behaviors				
Adult	Active	Active	Active	Active
Hate And Intolerance	Active	Inactive	Active	Active
Prevent	Active	Active	Active	Active
Proxy Filtering	Active	Active	Active	Active
Violence	Active	Inactive	Inactive	Active
Walled Garden	Inactive	Inactive	Inactive	Inactive
Youtube settings				
Youtube For Schools ID				
Safe Search				
Search settings				
Safe Search	Inactive	Inactive	Inactive	Inactive
Prefered Search Engine	google.co.uk			google.co.uk

List Overview

We mentioned earlier that your Lists operate independently from Profiles or Locations. On this page you can view, edit or remove your Lists. You can also create and populate new lists by clicking the on the relevant section. To apply a newly created list to a Profile, go to the settings within that profile.



Custom Reclassifications

This page allows you to manually reclassify a domain or sub domain to a new category and lists any domains / that have previously been reclassified on your account.

To add or check a classification, click the . Type in the address in the domain field and SurfProtect will show you how that domain is currently classified and give you the option to change it. You can also remove your custom classification by clicking the .

Diagnostic Tools

Domain Classification

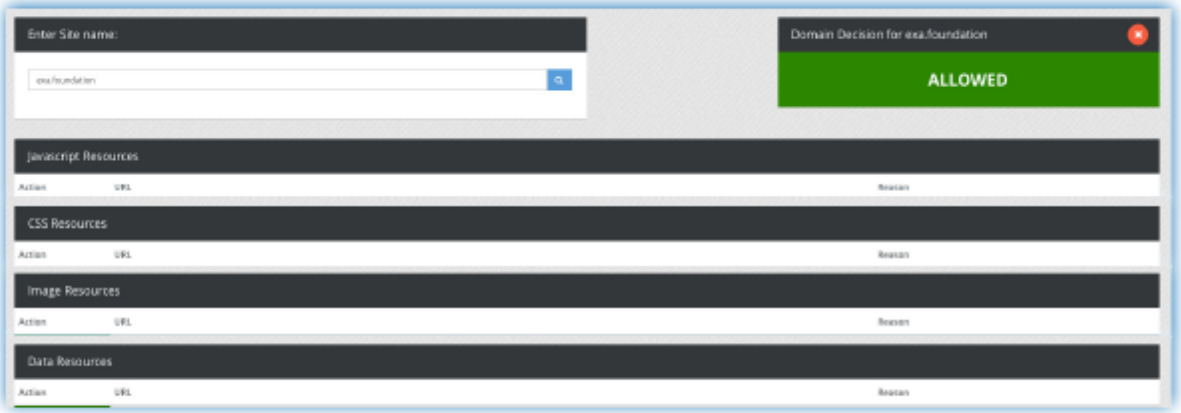
Accessible on any page, this overlay pop-up is the same as the tool for Custom Reclassifications and allows the checking and changing of a domain's classification.

Domain Doctor

A new feature of SurfProtect is the Domain Doctor.
This can be used when a site is blocked on your connection and you don't know why or it does not appear as you would expect.

The Doctor analyses all aspects and content of the site and shows you which elements are being blocked. From here you can allow any blocked element so that it displays correctly.

Submit the site you want diagnosing and hit the search button. The Doctor returns the decision that your filtering policy has made. From this page you can override this decision by clicking on the or on the relevant row. If any element returns 'Pending' it means that our classifiers are currently analysing the element - this is done live and in most cases clicking the icon will return a decision.

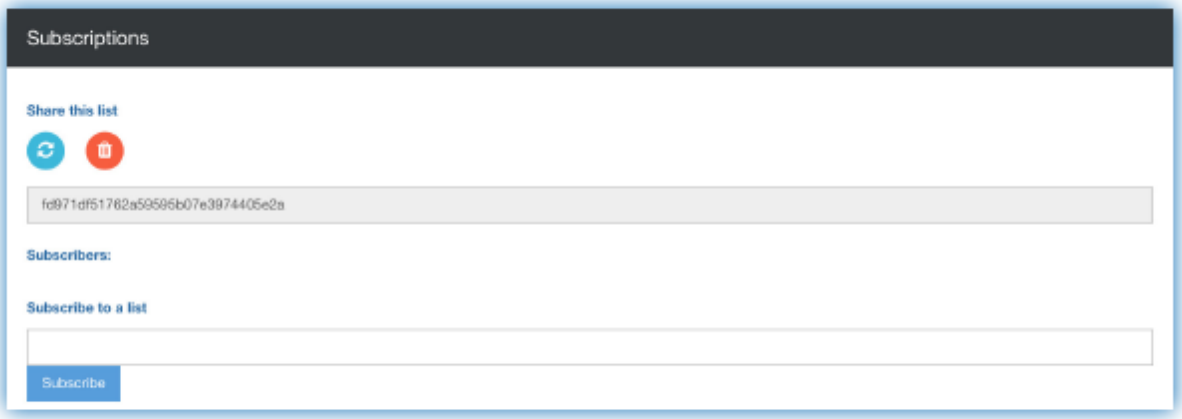


List Subscriptions

Sharing Allowed and Blocked Lists Across Schools

If you manage the SurfProtect settings for a number of schools, or are part of an MAT or cluster, you may want to share the same Allowed and Blocked URL Lists with each school within this group. With our new List Subscription feature, it is easier than ever before to apply one list to multiple schools.

At the top of each Allowed or Blocked List, you will see the Subscriptions option below.



To share a List with a school, simply send them the code generated in the top field – they can then paste this into the 'Subscribe to a list' box. Once they have clicked the 'Subscribe' button, the List will be applied to that profile. Alternatively, if you have access to the school's SurfProtect profile, you can perform these actions on their behalf.

In subscribing a school to a specific List, you ensure that they will automatically receive any subsequent updates or amends you may make to it in the future – so it's easier than ever before to manage and maintain Allowed and Blocked Lists across multiple schools.

> **Note:**
> As the subscribe feature is applied per List, if a school has multiple profiles using one List you will only need to paste the code into one of these and all others will simultaneously receive it.

If you would like to delete a List's code to prevent it being shared without authorisation, you can do so by clicking on the . This will mean that it can no longer be shared with any new users, but all existing subscribers will continue to receive any updates or changes made. To generate a new code for a List, click on the icon.

To remove a subscriber, click the icon beside their name and they will no longer have the List applied to their profile/s. All schools currently subscribed to a List are displayed at the top of the page, so that you have constant visibility over those using it.

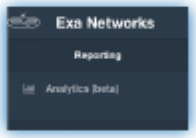
SurfProtect Analytics

SurfProtect Analytics provides you with an overview of the activity performed on your school's connection.

Analytics is currently most effective for SurfProtect Fusion customers due to its Active Directory integration enabling web activity to be attributed to the individual user. However, SurfProtect Cloud and Proxy users are able to view the top twenty most popular websites accessed on their network and rejected requests, as well search queries done over the HTTP protocol.

Getting Started

To access SurfProtect Analytics, simply click on the 'Analytics (beta)' section on the left hand side of your SurfProtect panel. This will open a new tab and show you all of your day's data so far (this will update every fifteen minutes to provide you with the most recent information).

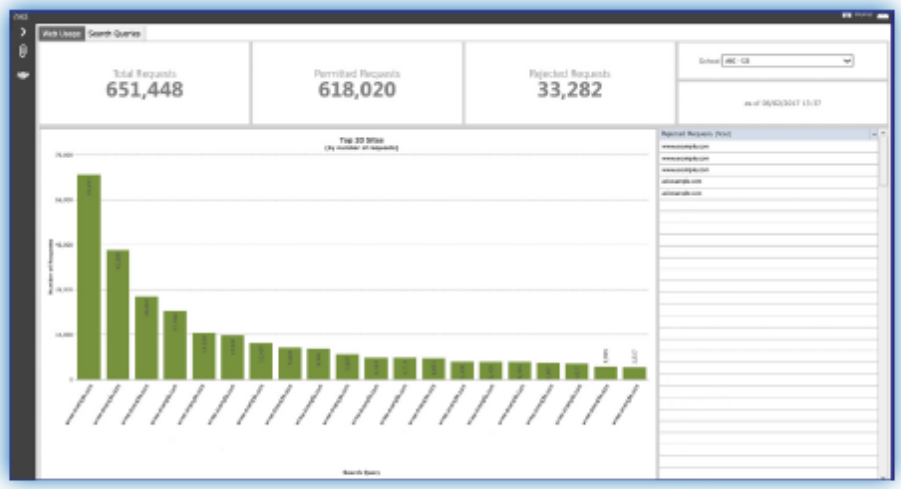


Analytics are divided into two sections - 'Web Usage' and 'Search Requests.' The one which is visible upon logging in is 'Web Usage', simply click between the tabs to alternate your view.

Web Usage

This screen provides an overview of the websites requested, the number of times they were accessed and which were blocked. The graph displays the top twenty most popular websites visited - for the large majority of schools, the number one site will typically be their chosen search engine. The list on the right hand side displays the web addresses that were blocked by your SurfProtect policy, you may notice that there are a high number of rejected requests which begin ad. These are generally pop-up advertisements which are blocked by default with SurfProtect.

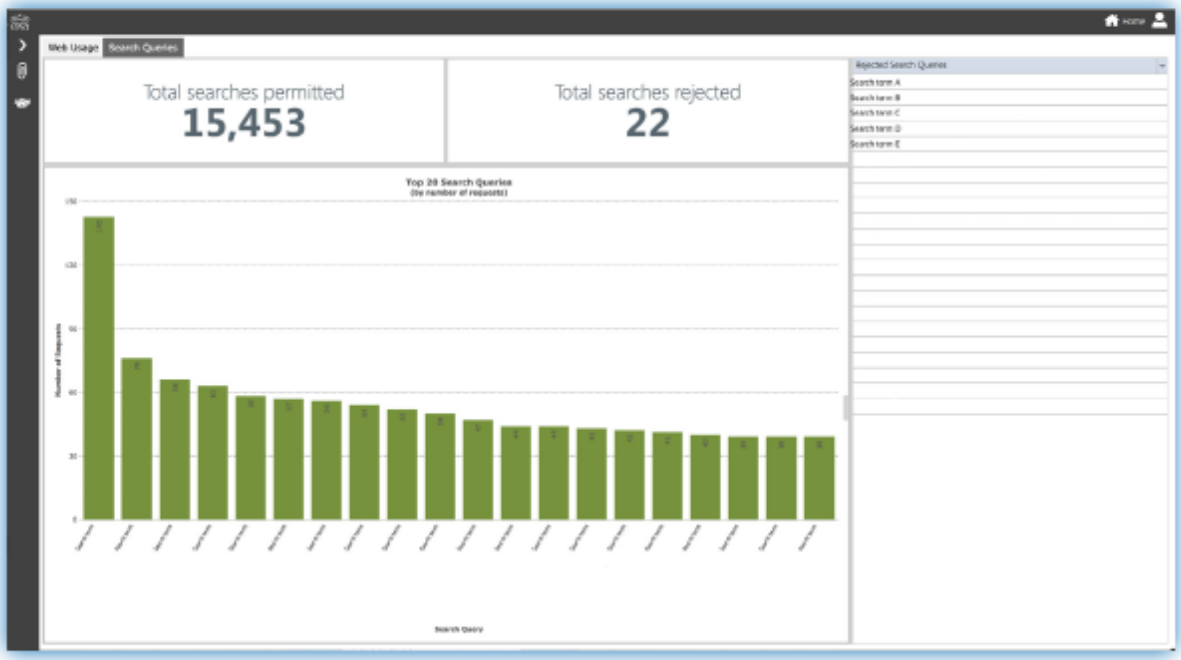
If you would like to see which student has requested a banned URL, simply clicking on the rejected request will bring up both their username and the timestamp that the attempt was made.



Search Queries

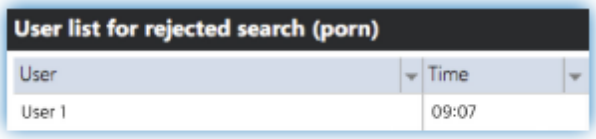
This screen provides you with details on the type of content students are searching for.

- The graph shows the top twenty most popular returned search queries, and the number of times they were requested.
- The 'Total searches permitted' is the number of search requests which were allowed according to your school's SurfProtect policy.
- The 'Total searches rejected' is the number of search requests which were not allowed as they contained words included in your SurfProtect blocked search term list(s).



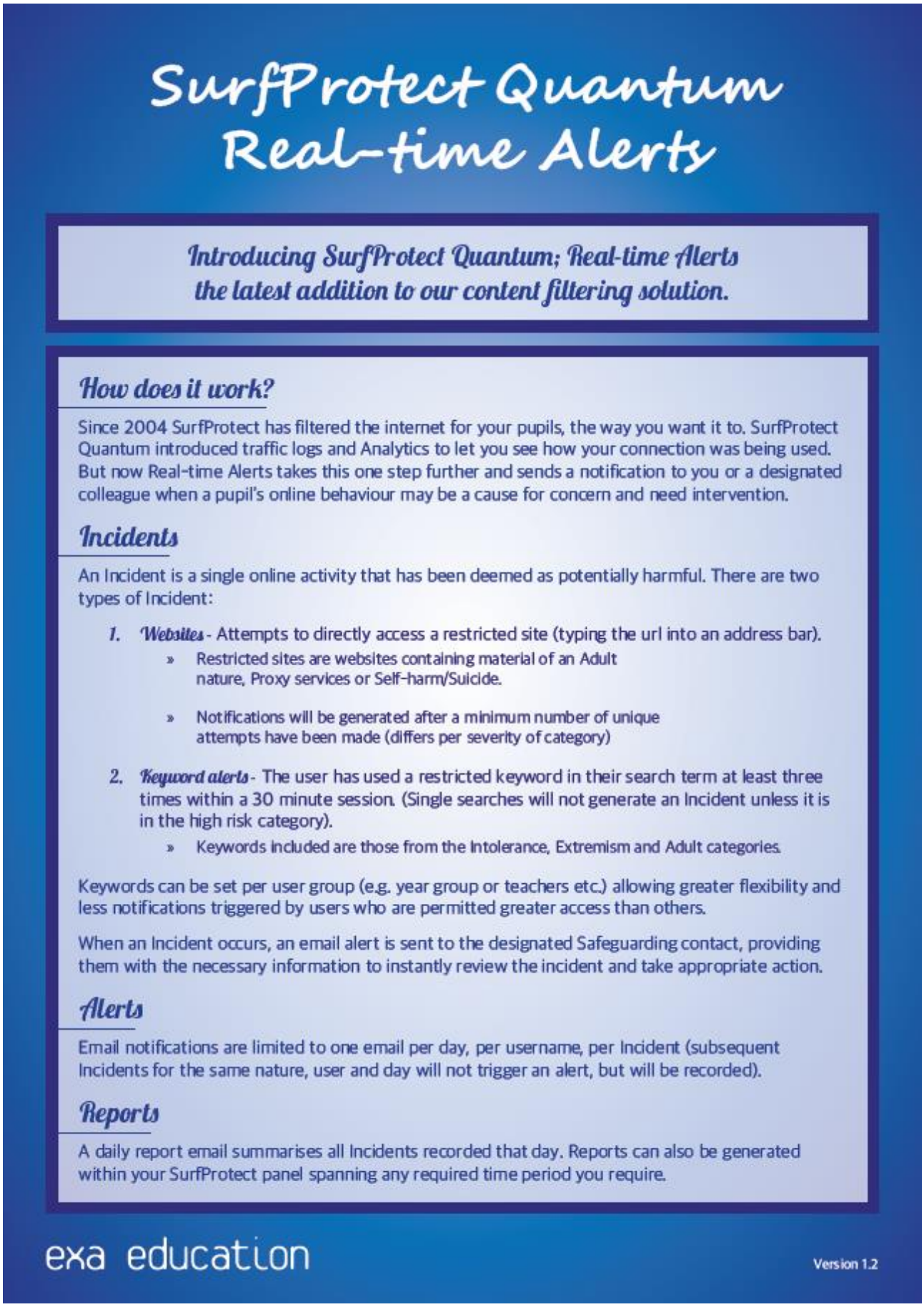
Identifying Inappropriate Activity

As with 'Web Usage', the right hand side bar displays rejected search queries and to find out which user performed the search at what time, you simply need to click on the query. Please note that as individuals are identified by integration with your school's Active Directory, the username will match that of the AD and therefore may not be immediately recognisable.



SurfProtect.co.uk | exa.education | 0345 145 1234

SurfProtect Quantum Real-time Alerts Overview



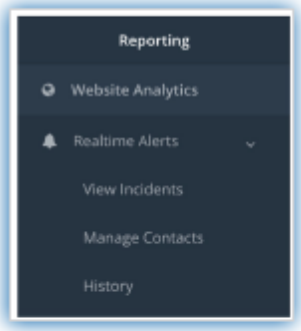

exa
SurfProtect
since 2004
Guide to the Real-time Alerts Panel
Version 1.1

SurfProtect Real-time Alerts User Guide

SurfProtect Real-time Alerts is a monitoring system that looks for specific types of behaviour when users are web browsing. When a set of requests within a given timeframe are identified as something that should be reported upon, an incident is created with those requests as events within it.

The interface on the panel allows a user to view and manage these incidents as they are reported.

Where do I find reports?



When viewing the SurfProtect panel, if the user has been granted access to view Real-time Alerts, a menu option under the Reporting area will be visible (as shown in the image).

From this menu users are able to view and/or manage three different aspects of Real-time Alerts; **Incidents**, **Contacts** and **History**.

If you are unable to see this menu this may be due to the following:

- Your user credentials are not associated with the ownership of the SurfProtect service.
- The user you are logged in with does not have sufficient access rights to view Real-time Alerts

Accounts and access

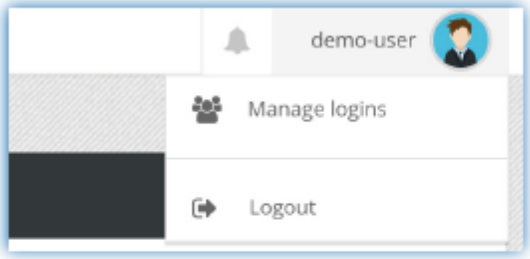
Due to the sensitive nature of the data available, specific access rights must be granted to access the panel. The ability to access Real-time Alerts can only be granted by an existing user of that account.

For example:

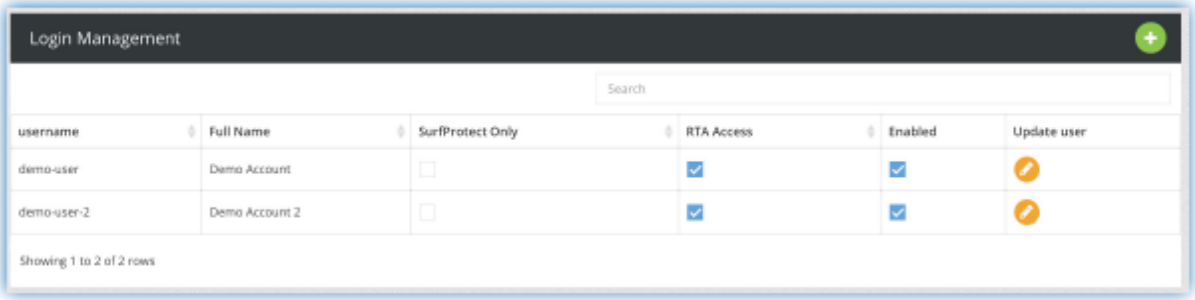
- If a user needs to be able to view your Real-time Alerts then the Admin user can either grant an existing user access or create a new user with access.

Managing logins

Once logged into the self administration panel, existing user logins for the account can be managed from the user menu in the top right hand corner.

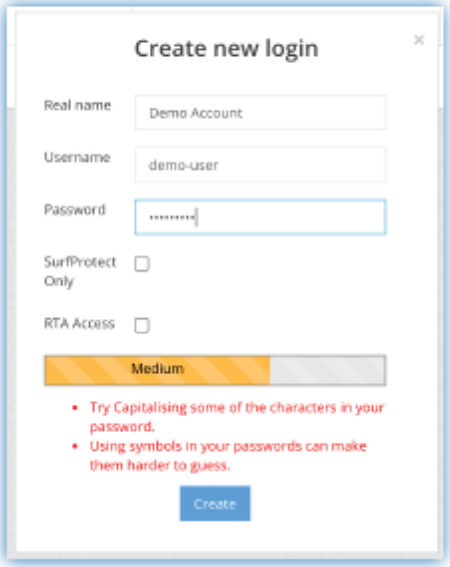


Selecting the 'Manage logins' menu option will navigate to show the list of all user logins for the account. This page then allows for the creating and updating of those users.



Creating new users

To create a new user account, and grant Real-time Alerts access, simply click the + in the top right corner of the Login Management table. This will open the user creation dialogue, which takes the following values:



- **Real name:** The full name of the given user.
- **Username:** The login username for the user, and will also be displayed on the panel after logging in.
- **Password:** The password for the new user, which must at least meet the medium strength requirements to be created.
- **SurfProtect only:** This flag only lets the user log in on the surfprotectpanel.exa.net.uk panel.
- **RTA Access (Real-time Alerts Access):** This flag allows the user to access the Real-time Alerts data for the account.

Granting/Removing access

For existing users, checking or unchecking the 'RTA Access' flag on the Login Management table will prompt to either enable or disable the ability for the user to access Real-time Alerts data on the panel.

Manage Contacts

This is the area where designated contacts for Real-time Alerts are setup and managed. A contact is defined as someone who should receive notifications about incidents (e.g. Safeguarding Officer/Lead). Each contact is made up of three parts:

- **Contact information:** First name and last name.
- **Contact method:** Email is the only available contact method currently. In future, alternative methods of contact may be developed.
- **Locations managed:** Identification of all Locations the User is to receive alerts for.

Adding a contact who does not already have a user profile will only generate the alert emails and will not grant access to the Real-time Alert area within the panel.

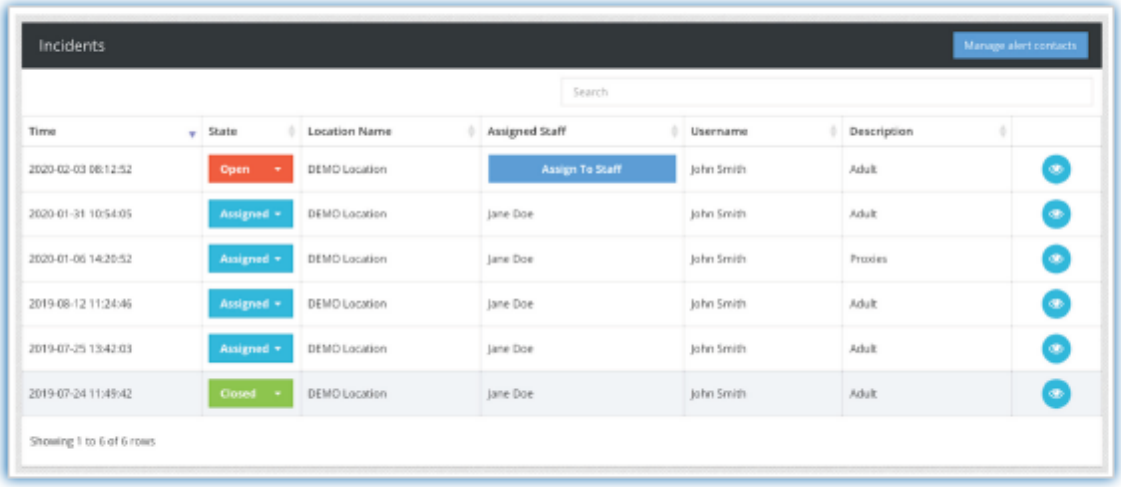
Incidents

An Incident is a single online activity that has been deemed as potentially harmful. There are two types of Incident

1. **Websites** - Attempts to directly access a restricted site such as websites containing material of an Adult nature, Proxy services or Self-harm/Suicide. Notifications will be generated after a minimum number of unique attempts have been made. The threshholds for the catagories are as follows:
    - Adult - 5
    - Proxies - 4
    - Suicide - 1
2. **Keyword alerts** - The user has used a restricted keyword in their search term at least three times within a 30 minute session. (Single searches will not generate an Incident unless it is in the high risk category).
    - Keywords included are those from the Intolerance, Extremism and Adult categories.

Keywords can be set per user group (e.g. year group or teachers etc.) allowing flexibility and less notifications triggered by users who are permitted greater access than others.

View Incidents



This overview lists all incidents which have occurred within the SurfProtect service.

At a glance, each incident row allows you to view when the incident began, it's current state, location name, name of assigned staff member, the username of the individual who generated the incident and a description of the category.

From here you can alter the state of an incident between Open, Assigned or Closed.

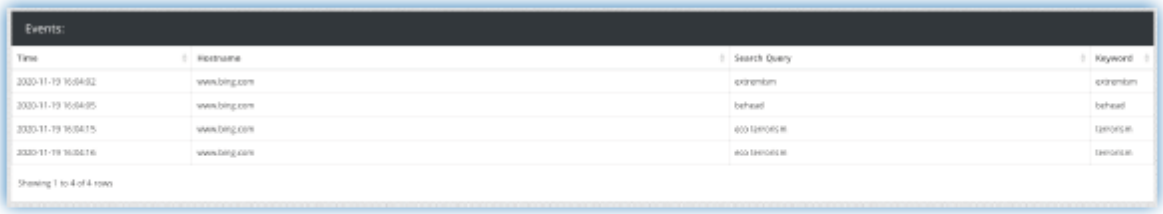
- Open: New, unassigned incident. In this state you have the option to assign the incident to a specific staff member.
- Assigned: Ongoing incident which is assigned to a staff member.
- Closed: An incident which has been deemed as complete.

Select the eye icon, to view any incident in further detail.

Viewing a specific incident

This gives a more detailed view of the incident as a whole, broken up into three specific sections:

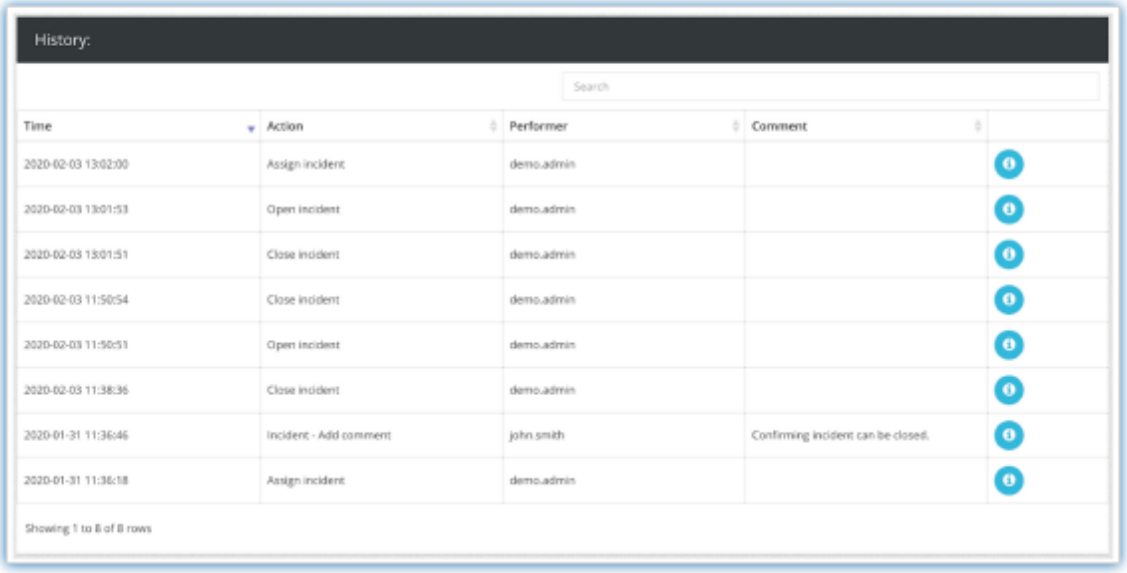
1. Viewing Incident - An overview of the incident, including a unique identifier, with the option to reassign the incident to a different user.
2. Comments - Lists all comments committed by Assigned Users. Each comment shows time, name of commenter and the comment itself. Select to add a new comment.
3. Events - A time log of all activity related to the incident.



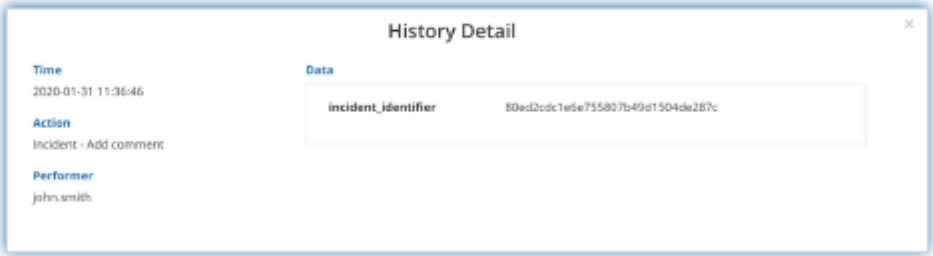
Each event is time stamped and provides the host that was visited. If the alert was raised due to a restricted keyword being searched then the search query and specific matched keyword will also be listed.

History

This section details all actions performed by users within the Real-time Alerts section of your panel.



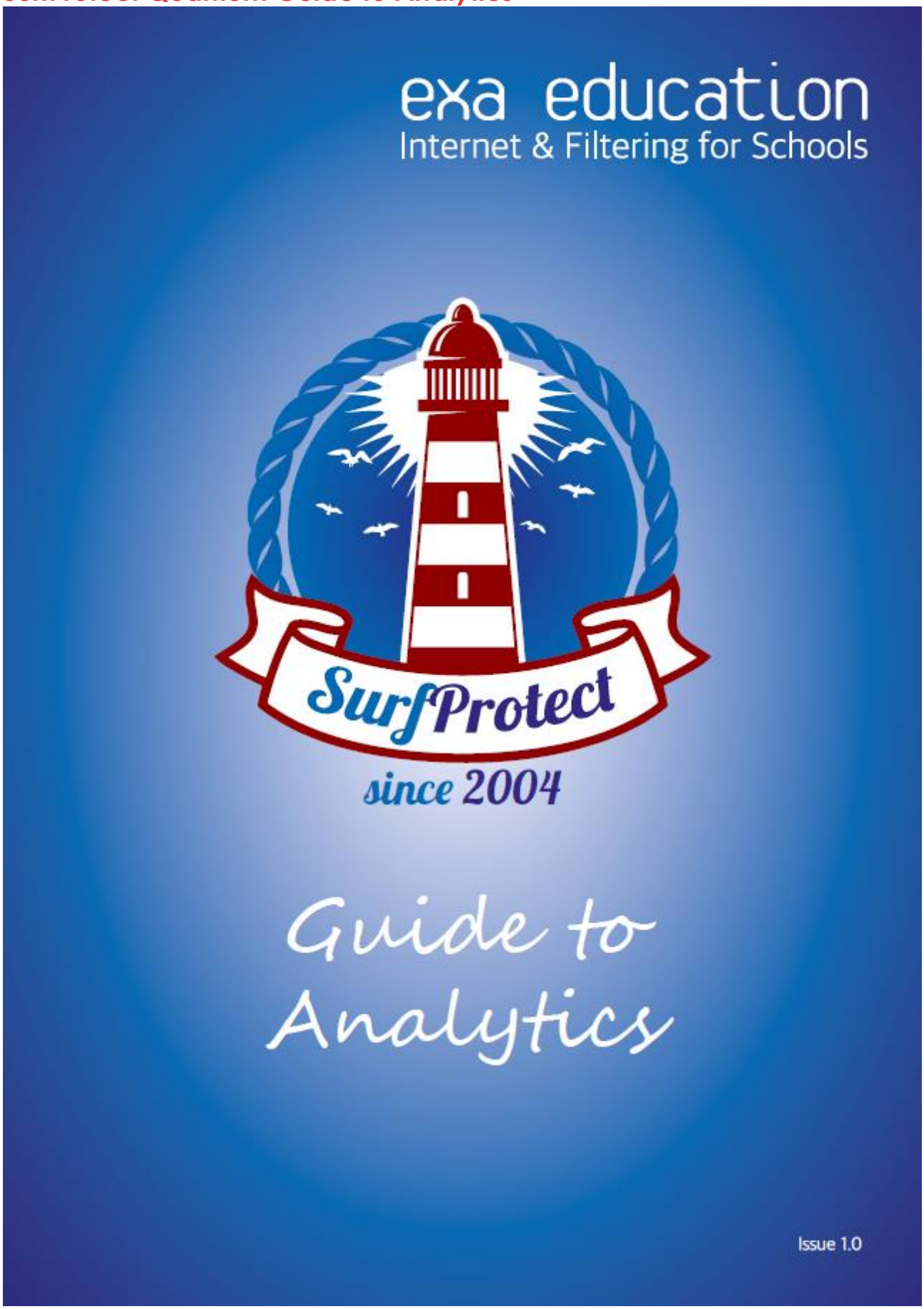
Each record can be viewed in more detail:



Each record details the time, action performed, user, unique identifier and any additional information available such as assigned staff etc.

If you have any questions please get in touch via helpdesk@exa.net.uk or give us a call on 0345 145 1234.

SurfProtect Quantum Guide to Analytics



Understanding Analytics...

With monitoring now forming a key part of a school's online safety requirements, we have worked tirelessly to introduce these features to our SurfProtect content filtering service. If you have previously purchased a Stormshield device, you'll be aware that you have always had access to a degree of reporting and visibility, however our SurfProtect Quantum service brings this capability to every user – and also introduces additional, brand new, features. In this guide, we will take a look at exactly what you can see in the SurfProtect Quantum reporting panel.

How Does It Work?

Located entirely in the cloud, SurfProtect Quantum does not require an on-site device to be configured and installed – you are even able to receive AD integration by simply installing an AD proxy. In doing this, your AD server is able to communicate with SurfProtect; as a result, every time a user visits a website, attempts to access a banned site, searches for blocked material, or simply enters an allowed search term, we are able to record this activity – ensuring that you have complete visibility over the online activity of each and every user within the school.

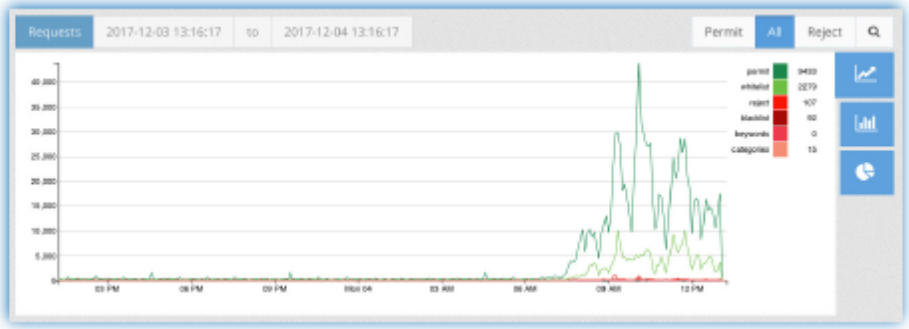
Our SurfProtect Fusion service utilises a Stormshield UTM device to provide AD integration, so this level of user reporting is also available to these schools.

If you do not wish to employ the AD integration aspect of SurfProtect Quantum, or are currently using our Cloud or Proxy services, you will still receive online analytics but will be unable to identify the individual user of any activity, and will instead only see the external IP an event is associated with.

So, what can you see?

The Big Picture

Upon logging into your SurfProtect Quantum panel, you will see a tab on the left hand side titled 'Website Analytics' – click on this, and you will be provided with a graphical overview of all activity performed on your school's internet connection in the previous twenty four hour period. This can then be selected to view filtered views of blocked, allowed, and complete traffic.



Key

- *Permit* – Websites and search terms which were allowed as they did not contain any restricted material or keywords
- *Whitelist* – Websites which have been explicitly allowed by the school
- *Reject* – The total number of all blocked requests
- *Blacklist* – Websites that the school has explicitly restricted access to
- *Keywords* – Search terms which contained words blocked by the school's 'Keyword' filtering
- *Categories* – Websites which were blocked as they belonged to a banned category

A Finer View

Beneath the graph, you will see a bar which provides a numerical representation of all activity performed over the last twenty four hours.

This is divided into four categories:

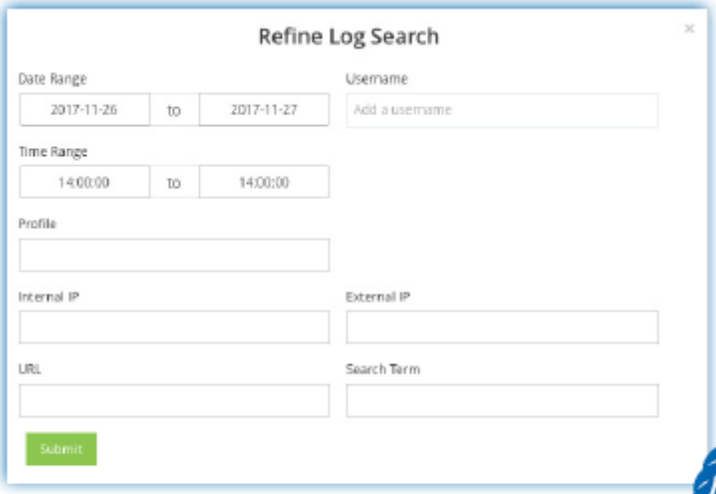
- *Activities* – This is where you will see every activity that has occurred; including every website requested, every download made, and every image viewed etc.
- *Unique Activities* – If a website or activity has occurred more than three times it will be listed here just once, providing you with a more concise view
- *Searches* – Search terms entered into Google, or alternative search engines, will be visible here
- *Unique Searches* – If a search term has been entered more than three times, it will again be displayed here just once

Clicking on the relevant button will then provide a list of the individual actions within the category, and can again be filtered to display blocked, allowed, and complete traffic. For example, clicking on the 'Searches' tab and selecting 'Reject' as the filter will bring up a list like the one shown below:

Time	Username	Status	Host	Query	Profile		Decision Item
27-11-17 07:3...	example	reject	www.google.c...	porn	students - Ext...	search terms	Keyword: porn
27-11-17 07:4...	example	reject	www.google.c...	porn	students - Ext...	search terms	Keyword: porn

As you can see, we are able to identify the time the incident took place, the term that was entered, the Keyword which caused it to be rejected and, if AD integration has been enacted, the user that performed the search and the AD profile they are associated with.

When viewing this list with AD integration, you may notice that an individual has performed a search which raises concern. If this should happen, you are able to filter the data records to only display their web activity over a specified period of time. This is done using the 'Refine Log Search' feature shown below.



You are also able to perform this search for multiple users or, alternatively, see all the activity performed under an AD profile - such as Students, or even find out who has been searching for a specific term or attempting to visit a banned site.

SurfProtect.co.uk | exa.education | 0345 145 1234

Exa Foundation Learning Program

The Exa Foundation is part of Bradford based ISP, Exa Networks. Established in 2015, the Foundation has hosted a popular nationwide programme of physical as well as online events, conferences and festival workshops for learners, educators and digital makers of all ages.

The Foundation provides professional development to teachers and staff and publishes resources in response to identified needs.

In Spring 2022, we launched our new **'LEARNING PROGRAMME'** to develop a deeper understanding of connected technologies and promote their safe, secure and appropriate use.

THE EXA FOUNDATION SESSIONS ARE INCLUDED IN THE EXA CONNECTIVITY PACKAGE.

THE FOUNDATION IS AVAILABLE TO NON-EXA CUSTOMERS FROM £1,000 PER DAY.

Protect & Connect®

P1	**HELLO, IT'S ME.** Protect & maintain my identity *LO: Use technology safely, including protecting their online identity.*	C1	**VICTORIAN INTERNET** Explain how and why the internet was created *LO: Understand the development of the internet and WWW, and the opportunities they offer for communication and collaboration.*
P2	**WALLS HAVE EARS** Take steps to proactively manage my privacy *LO: Use technology safely, including protecting their privacy.*	C2	**CONNECTING THE DOTS** Justify reasons for using a network *LO: Understand how computer networks can provide multiple services and the opportunities they offer for communication and collaboration.*
P3	**YOU CAN'T UNSEE IT** Act against harmful content & unwelcome contact *LO: Recognise inappropriate content, contact and conduct, and know how to report concerns.*	C3	**ABOUT THE SIZE OF IT** Measure and compare internet speed & bandwidth *LO: Understand how data is stored, represented and transmitted in the form of binary digits.*
P4	**ON YOUR GUARD** Respond appropriately to malicious behaviour & criminal activity *LO: Recognise inappropriate content, contact and conduct, and know how to report concerns.*	C4	**PLAYING BY THE RULES** Explain why protocols are needed to govern the internet *LO: Understand how computer systems communicate with one another.*
P5	**FAKE NEWS** Discern unreliable content & false information *LO: Recognise inappropriate content and conduct, and know how to report concerns.*	C5	**WEB DEVELOPMENT 101** Use free tools to develop content for the web *LO: Use software to design and create content to accomplish given goals.*
P6	**INFORMATION SECURITY** Identify systems that protect me & understand how *LO: Understand the hardware and software components that make up computer systems, and how they communicate with one another and with other systems.*	C6	**THIS IS FOR EVERYONE** Defend the morals & ethics of the internet & WWW *LO: Recognise the internet as a source for both good and evil.*

Learning Objectives for all sessions are purposefully linked to UK National Curriculum requirements and have the flexibility to be adapted to **suit audiences in KS2, KS3, KS4, KS5 or alternatively as part of a CPD programme** for staff. **Each session lasts from 45 minutes up to a half day.**

The exa Foundation

WITH GREAT POWER COMES GREAT RESPONSIBILITY

The introduction and development of the internet and WWW has enabled collaboration on a global scale. How else might advances in science, technology & medicine have ever happened?

The ability to connect instantly with others presents extraordinary potential to educate and problem solve worldwide, but at the same time opens up opportunities for crime and terror.

Our programme offers engaging experiences for schools that:

- CAPTIVATE INTEREST THROUGH ENGAGING **STORYTELLING**
- DEVELOP CRITICAL THINKING THROUGH **DISCUSSION**
- EXTEND THE USE OF CORRECT TECHNICAL **VOCABULARY**
- PROVIDE COLLABORATIVE **PROBLEM SOLVING** ACTIVITIES
- CULTIVATE POSITIVE ATTITUDES & **DIGITAL SKILLS** FOR THE WORKPLACE

HOW TO FIND US

exa.foundation

0345 145 1234

info@exa.foundation

@exafoundation

exafoundation

TO BOOK A SESSION VISIT

https://exa.is/booksession

exa

The Exa Foundation, 100 Bolton Road, Bradford, BD1 4DE
Registered Company Number: 04922037
The Exa Foundation is a branch of Exa Networks Limited