exa education
Internet & Filtering for Schools

Keeping children safe in education: Online safety and SurfProtect®

On September 5th, 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 can help your school to meet these new guidelines, and implement the most effective & appropriate filtering policy possible - ensuring that both staff and students are protected from the many dangers present online.

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

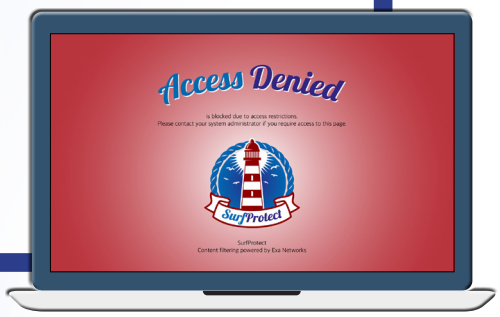
You can also learn more at **www.surfprotect.co.uk**.

1) Filtering Content

SurfProtect 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'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 is now 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. Although a very important issue, the Prevent duty guidance can be a little confusing in its requirements and expectations of schools.

SurfProtect 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 also provides you with the 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.

3) Reporting Content

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

Our SurfProtect Fusion service works in conjunction with an Exa Education supplied-and-managed firewall to enable you to view reports of all activity taking place on your school's internet connection – from which sites are being requested, which are most frequently viewed or blocked, 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, whilst also monitoring the way in which your internet service is being used.

SurfProtect Fusion provides real-time visibility on all live traffic as well as historical logs of all usage, so you can be assured that you have total visibility. We also have new reporting and monitoring tools in development – to be launched shortly – to ensure all SurfProtect users are able to benefit from this ability!

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, 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.

If you are using our SurfProtect Fusion service, you can create filtering profiles which are even more user-specific. With its Active Directory integration feature, it is possible to create separate policies for groups, subject classes, and even individual users. And, with our brand new 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.

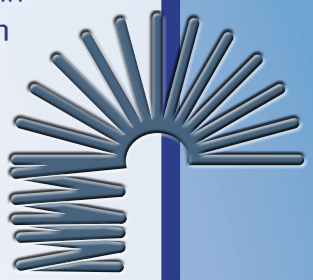
With SurfProtect, it is possible to ensure that every device – whether static or mobile, owned by the school or the student – receives the same level of protection. This is because SurfProtect implements network-level filtering, which means that all traffic on the school's internet connection is filtered – 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 the therefore SurfProtect – 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'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's web-based portal means that authorised staff members can review and edit filtering policies any time they're connected to the Internet – giving you total convenience, and making sure that you're always in control of your content filtering. And, SurfProtect 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.



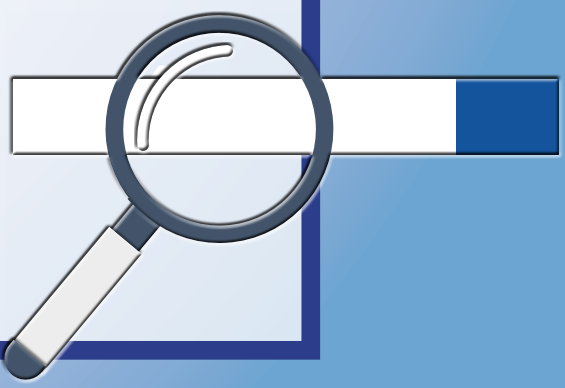
7) Search Term Filtering

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's brand new 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 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 one click, 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 and the posting of comments – helping to prevent pupils from requesting offensive videos or writing inappropriate feedback.



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

SurfProtect
since 2004