SurfProtect®

KCSIE Guidelines

Issue 7.0
Sep. 2023

Complying with DfE Guidelines

On September 1st 2023, updated guidelines issued by the Department for Education for 'Keeping Children Safe in Education' came into effect. One key part of these guidelines is online safety, and how schools must implement appropriate filtering and monitoring systems to ensure that students are effectively protected whilst online.

Staying safe online

The KCSIE guidelines categorise online safety as comprising the following four key areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material;
- **Contact:** being subjected to harmful online interaction with other users; and
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams

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: exa.is/appropriate

This guide explains how SurfProtect Quantum and 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 online dangers.

More than just filtering...

As highlighted in the KCSIE guidelines, both teachers and students should be provided with effective **safeguarding training** alongside the filtering and monitoring of online activity.

Created in October 2015, The Exa Foundation is part of Exa, and is dedicated to providing schools with the advice, resources and guidance needed to embrace everything technology has to offer - safely.

The Exa Foundation provides **e-safety courses** for teachers, 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 customer, you receive access to this - and all other Exa Foundation services - completely free of charge.

Learn more at exa.foundation

SurfProtect's filtering policy

The UK Safer Internet Centre specifies the types of content and communication a school should restrict access to. In blocking these categories, detailed below, a school ensures that both staff and students are protected from exposure to offensive and illegal material whilst online.

SurfProtect automatically implements a default filtering policy which prevents access to the web categories detailed by the UK Safer Internet Centre, alongside a number of other inappropriate topics. However, it is also incredibly easy to build on this default 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.

Content	Definition	Blocked by default?
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.	Yes. SurfProtect's 'Intolerance & Hate' category includes 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.
Gambling	Enables gambling	Yes. The 'Gambling' category is blocked by default.
Malware/Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content.	Yes. The categories 'Hacking', 'Spyware' and 'Virus Worm Infected' are blocked by default.
Pornography	Displays content of sexual acts or explicit images.	Yes. SurfProtect's 'Adult/Sexually Explicit' category is automatically restricted.
Piracy and copyright theft	Includes illegal provision of copyrighted material.	Yes. SurfProtect automatically prevents access to 'Illegal Filesharing' and 'Peer to Peer' sites.
Self Harm	Promotes or displays deliberate self harm (including suicide and eating disorders).	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.

KCSiE Requirements

There are a number of questions that the UK Safer Internet Centre recommends asking your filtering provider to ensure the system you are supplied with meets the new Keeping Children Safe in Education guidelines. Here, we'll highlight what you need to know about SurfProtect Quantum and Quantum+.

1. **Does the filtering system offer the ability to vary filtering strength appropriate to age, vulnerability and role?**

With SurfProtect, you can allow different year groups and job roles 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'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.

2. **To what extent and ability does the filtering system identify and manage technologies and techniques used to circumvent it, e.g. VPN and proxy services and DNS over HTTPS?**

To combat the use of proxies, when a user visits a URL such as 'www.google.co.uk', the entire URL is inspected to prevent restricted content being accessed including a blocked domain address within the Google URL path (this is typically enacted through the use of Google Translate). You are also able to restrict access to a number of proxies by blocking the category 'Proxies and Translators' in your online portal.

To prevent VPNs being utilised to bypass SurfProtect, we advise that schools restrict the ports and protocols typically used by the technology, such as port 1723, on their firewall. If you receive a managed firewall from Exa, VPN blocking will be turned on as a default.

However, advanced VPN technologies which are specifically designed to circumvent filtering services mask their traffic and do not use 'expected' ports and protocols and as a result, can be utilised to bypass SurfProtect on occasion. We therefore advise that schools operate stringent cyber security policies which prohibit students from implementing these technologies such as Device Management for example, to ensure any unverified programmes cannot be installed.

DNS is also filtered by SurfProtect. When a DNS lookup is made, the request is intercepted and sent to the SurfProtect DNS servers. Additionally SurfProtect has the ability to filter DNS itself, this includes DNS over HTTPS.

3. **Does the filtering system provide the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content?**

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.

4. **Does the filter system log any changes enabling an audit trail that ensures transparency and individuals are not able to make unilateral changes?**

There is an audit trail in SurfProtect which shows what changes have been made.

5. **In addition to URL or IP based filtering, to what extent is content analysed as it is streamed to the user and blocked, this would include AI generated content. For example, being able to contextually analyse text on a page and dynamically filter.**

When a URL is visited for the first time it is downloaded and its content is analysed by SurfProtect. These URLs are revisited on a regular basis, and the content re-analysed.

6. **Does the filtering provider publish a rationale that details its approach to filtering with classification and categorisation as well as over blocking?**

SurfProtect uses a range of technologies, bolstered by human verification, to accurately classify web content with all categories that apply. Sensible defaults are applied to new profiles to restrict access to offensive and inappropriate material, and schools are provided with simple tools to support the creation of custom policies that permit access to all desired types of content.

Support for multiple types of profiles ensures that content can be selectively blocked or allowed as is appropriate for different types of user, without impeding other people within the school.

Reclassifications are automatically synchronised between data centres so all users immediately benefit from manual intervention in case overblocking is detected. Custom categories or overrides on block and allow lists can also be employed by an administrator to immediately provide or restrict access to specific requested content within the entire school.

7. **Does the filtering system have the ability to provide the deployment of central policy and central oversight or dashboard identification?**

SurfProtect's online web portal allows administrators to deploy a central policy for all groups, users, and devices, whilst providing 360° visibility over all settings and activity performed on the connection.

As a cloud-based system, it can also be deployed across multiple sites, and controlled either across all, individually, or a select number, depending on the requirement. A subscription feature is available to use which allows a centralised filtering policy opt-in to be created between different sites/groups. Any changes made centrally will then be applied to all subscribed schools/groups. This gives the benefit of central management or alignment without handing over full control of the system, particularly helpful for MATs.

8. **Does the filtering system have the ability to identify users?**

SurfProtect offers a number of options for relating web traffic with the user who generated it.

This is achieved either through Active Directory integration or the use of Quantum+'s Captive Portal, which allows SurfProtect to relate traffic to the users in Active Directory, Google Workspace and Azure Tenants.

9. **To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)?**

SurfProtect filters web traffic at a network level, this makes the service agnostic of how web requests are made and able to filter requests from browsers, mobiles and applications.

10. Does the filtering system have the ability to manage relevant languages?

SurfProtect blocks set keywords in popular languages used in the UK by default such as:

- French
- German
- Spanish
- Polish
- Romanian
- Panjabi
- Urdu

And also automatically enforces SafeSearch on all major search engines to ensure that inappropriate search terms cannot be entered in any language.

11. Is the filtering applied at the network level i.e., not reliant on any software on user devices?

Located entirely in the cloud, SurfProtect performs network-level filtering. This means that all traffic on a school's internet connection can be filtered, regardless of the machine or device used to access it.

12. Does the filtering system provide the ability to report inappropriate content for access or blocking?

As all users have complete control over which content is allowed or blocked, inappropriate sites can be reported to the system's administrator's and immediately acted upon.

Alternatively, if you think a site has been incorrectly classified by SurfProtect, we encourage that this is reported to our team through the technical support HelpDesk or any other contact method.

13. Does the system offer clear historical information on the websites visited by your school's users?

SurfProtect Analytics records all web requests that are filtered through the SurfProtect service.

With the use of Active Directory integration, or Quantum+'s Captive Portal, these Analytics also include the associated user information when it is available.

With SurfProtect Analytics, you are also able to view reports of all online activity performed on your network. Compiling and storing this data for 3 month periods (1 year with Quantum+) 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 can request a physical record to reference.

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 or extremist 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 extremist or 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 and 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 Counter Terrorism Internet Referral Unit (CTIRU) 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.

SurfProtect Quantum

We designed and build our content filtering platform, SurfProtect Quantum, to fulfil Keeping Children Safe in Education (KCSiE) and The Prevent Duty filtering guidelines in the most cost effective way. SurfProtect 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 schools now providing their pupils with portable learning devices or enabling BYOD environments, filtering requirements have changed. To meet this needs we 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.

Both SurfProtect products work in conjunction with Securus and Smoothwall Monitor to provide a comprehensive solution to suit your requirements.

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	✓	✓
Works with any OS and web browser (browsers <5 years old)	✓	✓
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 filtering requirements of DfE KSCiE, Prevent Duty and Ofsted	✓	✓