SurfProtect®

DFE Guidelines

Issue 7.0
Nov. 2022

Complying with DfE Guidelines

On September 3rd 2018, 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 C, pp. 92-94), 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 three 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.

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 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.

exa.foundation provides an **e-safety course** 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 *www.exa.foundation*

*'Whilst filtering and monitoring are an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a **whole school approach** to online safety.'*

Keeping Children Safe In Education, September 2018

The things you need to know

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 Quantum 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 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.

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.
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.

The important questions

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 the ones you need to know, whilst also discussing how SurfProtect Quantum meets the updated standards for September 2018.

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

   With SurfProtect Quantum, 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 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.

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?**

   SurfProtect Quantum actively works to prevent the system being circumvented. To combat the use of proxies, when a user visits a URL, such as www.google.com, the entire URL is inspected to prevent restricted content being accessed through 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 Quantum, we advise that schools restrict the ports and protocols typically used by the technology, such as port 1723, on their firewall. 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 Quantum on occasion. We therefore advise that schools operate stringent cyber security policies which prohibit students from implementing these technologies through the use of USB sticks, for example.

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 Quantum'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 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.

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

SurfProtect Quantum 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.

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

SurfProtect Quantum'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.

6. **Does the filtering system have the ability to identify users?**
   With SurfProtect Quantum's Active Directory integration feature, you are able to identify individual users and their online activity.

7. **To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)?**
   SurfProtect Quantum provides an 'Application Control' feature which allows users to block or allow entire applications - working across the application layer, not just via web browser delivered content.

8. **Does the filtering system have the ability to manage relevant languages?**
   SurfProtect Quantum automatically enforces SafeSearch on all major search engines to ensure that inappropriate search terms cannot be entered in any language.

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

10. **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 Quantum, we encourage that this is reported to our team through the technical support HelpDesk or any other contact method.

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

    With SurfProtect Analytics, you are also able to view reports of all online activity performed on your network. Compiling and storing this data for one 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 can request a physical record to reference.

We hope this guide has been helpful, and if you like more information on SurfProtect Quantum, please don't hesitate to get in touch with a member of our team on **0345 145 1234** or at *sales@exa.net.uk*