



SurfProtect®

Compliance with Education Guidelines

What guidelines do schools need to meet?

Filtering requirements sit across a number of guidelines, which can make them difficult to navigate. This document brings clarity to how SurfProtect supports you in meeting those responsibilities.

Keeping Children Safe in Education

KCSiE statutory guidance reinforces that schools and colleges must have appropriate filtering and monitoring systems in place as part of their safeguarding duties. It refers to the DfE filtering and monitoring standards and the UKSIC guidelines which detail what is required when it comes to appropriate filtering.

DfE filtering and monitoring standards

This is one of the six core standards now published by the DfE. You should be meeting this standard now if possible, working towards meeting all six by 2030.

Technical requirements to meet the standard:

The Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU) provide lists of illegal websites that filtering providers can block as part of their service, known as blocklists. Schools and colleges must make sure these blocklists are implemented with their filtering solutions. Filtering solutions must be designed so that these blocklists cannot be disabled, overridden, or altered by any user in a school, college, multi-academy trust (MAT), local authority or any other responsible body, including system administrators, at any level.

Also make sure that your filtering provider is:

- ✓ a member of IWF
- ✓ signed up to CTIRU
- ✓ regularly updating blocklists based on information from IWF and CTIRU

Some schools and colleges may want to block additional, inappropriate content that their filtering system does not automatically block. Your system should allow you to add this content locally. Any additions should not disrupt or affect teaching and learning.

Your filtering system should be active, up to date and applied to all:

- ✓ school or college-managed devices, including those taken off-site
- ✓ unmanaged devices under a bring your own device (BYOD) scheme
- ✓ guests who have access to the school internet

Devices that are not school or college-managed, should be on a separate virtual network. Check with your provider to find out whether your filtering system:

- ✓ identifies and appropriately filters all internet feeds, including any backup connections and portable wifi devices
- ✓ is appropriate for the age and ability of the users
- ✓ is suitable for educational settings
- ✓ identifies multilingual web content, images, common misspellings and abbreviations
- ✓ provides alerts when web content of concern has been blocked
- ✓ blocks technologies and techniques that allow users to get around the filtering, such as VPNs, proxy services and end-to-end encryption methods

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the SLT or the designated safeguarding lead.

Your filtering systems should allow you to identify, as a minimum:

- ✓ device name or ID, IP address, and where possible, the individual
- ✓ the time and date of attempted access
- ✓ the search term or content being blocked

If the filtering provision is procured with a broadband service, ask your broadband provider how it meets these requirements.

UKSIC

The UK Safer Internet Centre publishes guidance as to what appropriate filtering and monitoring should look like for schools, and invites all providers to self-certify their systems using a checklist. We update our certification whenever we make any changes that effect our response or the guidelines are updated. You can see our responses on the following pages.

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.

Illegal Content

As part of the Online Safety Act there is now a defined list of illegal content that platforms (such as social media site) need to protect users from. These categories are now included under the UKSIC as content that should be blocked by default and not able to be disabled by anyone at a school.

Content	Definition	Blocked by default?
Child Sexual Abuse	Content that depicts or promotes sexual abuse or exploitation of children, which is strictly prohibited and subject to severe legal penalties.	Yes. CSAM falls under the IWF list which is always blocked and impossible to remove.
Controlling or Coercive Behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts	Yes. SurfProtect defines a "Controlling or Coercive Behaviour" category that users cannot opt out of blocking.
Extreme Sexual Violence	Content that graphically depicts acts of severe sexual violence, intended to shock or incite similar behaviour, and is illegal under UK law.	Yes. SurfProtect defines a "Extreme Sexual Violence" category that users cannot opt out of blocking.
Extreme Pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.	Yes. SurfProtect defines a "Extreme Pornography" category that users cannot opt out of blocking.
Fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.	Yes. SurfProtect defines a "Fraud" category that users cannot opt out of blocking.
Racially or Religiously Aggravated Public Order Offences	Content that incites hatred or violence against individuals based on race or religion, undermining public safety and cohesion.	Yes. SurfProtect defines a "Racially or Religiously Aggravated Public Order Offences" category that users cannot opt out of blocking.
Inciting Violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.	Yes. SurfProtect defines a "Inciting Violence" category that users cannot opt out of blocking.
Illegal Immigration and Smuggling	Content that promotes or facilitates unauthorised entry into a country, including services offering illegal transportation or documentation.	Yes. SurfProtect defines a "Illegal Immigration and People Smuggling" category that users cannot opt out of blocking.
Promoting or Facilitating Suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.	Yes. SurfProtect defines a "Promoting or Facilitating Suicide" category that users cannot opt out of blocking.
Intimate Image Abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.	Yes. SurfProtect defines a "Intimate Image Abuse" category that users cannot opt out of blocking.
Selling Illegal Drugs or Weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.	Yes. SurfProtect defines a "Selling Illegal Drugs or Weapons" category that users cannot opt out of blocking.
Sexual Exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.	Yes. SurfProtect defines a "Sexual Exploitation" category that users cannot opt out of blocking.
Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.	Yes. SurfProtect blocks websites on the CTIRU list, users cannot opt out of this behaviour.

Exa have also been Internet Watch Foundation members since 2005, and block access to the following lists by default with no ability to disable: IWF (checking the API multiple times a day for updates), CTIRU (Counter Terrorism Internet Referral Unit) and PIPCU (Police Intellectual Property Crime Unit). SurfProtect also enforces PDNS (Protective Domain Name Service) filtering, provided by NCSC (National Cyber Security Centre).

Inappropriate Content

See below how SurfProtect manages the defined list of inappropriate content from UKSIC.

Content	Definition	Explanation
Gambling	Enables gambling.	SurfProtect has a 'Gambling' category, which is blocked by default.
Hate Speech/ Discrimination	Content that expresses hate or encourages violence towards a person or group based on something such as disability, race, religion, sex, or sexual orientation. Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010.	This content falls under the 'Intolerance and hate' category, but may also fall under 'Criminal Activity' or 'Tasteless & Offensive' categories. Social Media sites are also likely to contain this content, which is covered by the 'Social Networking' category. This is blocked by default.
Harmful Content	Content that is bullying, abusive or hateful. Content which depicts or encourages serious violence or injury. Content which encourages dangerous stunts and challenges; including the ingestion, inhalation or exposure to harmful substances.	This falls under a range of categories such as the 'Violence' category, 'Criminal Activity' or 'Intolerance & Hate'. Harmful content could be found anywhere such as Social media. Along side blocking related categories and search-term based filtering, SurfProtect also provides filtering settings to help cover these areas by implementing Safe-search and Youtube restricted mode.
Malware/Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content.	SurfProtect uses PDNS from NCSC to block access to known malicious websites and cyber-security threats. Where any content is not blocked by PDNS, it will fall under the categories 'Hacking', 'Phishing/Online Fraud', 'Spam URLs' or 'Spyware', all of which are blocked by default.
Mis/Disinformation	Promotes or spreads false or misleading information intended to deceive, manipulate, or harm, including content undermining trust in factual information or institutions.	SurfProtect has a 'Mis/Dis Information' category, which is blocked by default.
Piracy and copyright Theft	Includes illegal provision of copyrighted material.	SurfProtect has an 'Illegal Filesharing' category that is blocked by default.
Pornography	Displays content of sexual acts or explicit images.	SurfProtect has an 'Adult / Sexually Explicit' category that is enabled by default. We also have an 'Intimate Apparel/Swimwear' category that catches the less explicit, but still inappropriate, content.
Self Harm and Eating Disorders	Content that encourages, promotes, or provides instructions for self harm, eating disorders or suicide	SurfProtect has a 'Suicide & Self harm' category that is blocked by default. Our alerting system also analyses requests which fall into the 'Suicide & Self harm' category, or have identified searches related to this category, and generates alerts and emails to notify nominated contacts.
Violence Against Women and Girls	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.	The content falls under the 'Violence' category, but may be covered by other categories such as 'Criminal Activity' or 'Intolerance & Hate'.

SurfProtect's has a classification database of over 68 million domains, which are split into 61 distinct categories. We have manually-configured settings for over 150 thousand websites, reflecting 20 years of experience in web filtering. Per DfE guidance, customers are able to set their own categories, allowing them to tailor SurfProtect to the needs of their organisation's filtering requirements.

SurfProtect also applies search term filtering to a number of platforms such as Google, Bing, DuckDuckGo, Wikipedia and YouTube. We offer 10 'sensible default' lists of search terms that customers can use (such as words related to weapons, drugs and sex), in addition to allowing customers to define their own lists. These lists are available in the 10 most spoken languages in the UK.

Data Retention

SurfProtect Quantum allows customers to view the last 3 months worth of log history, whereas Quantum+ allows for 12 months. The identifying information available in the logs depends on how a customer has configured their SurfProtect service, for their own requirements. At minimum, this will be an external IP address, but can also include internal IP addresses and usernames from any supported user identity provider, such as Windows Active Directory, Google Workspace or Microsoft Entra ID (formerly known as Azure Active Directory).

Over Blocking

SurfProtect's default setup provides 'sensible defaults' such as Blocking illegal and inappropriate content, enabling safe search on search engines, YouTube restricted mode and blocking inappropriate search terms. Currently, by default, we block AI content as we develop more solutions to combat this new landscape, making sure we are in the best position to protect our users.

All these filtering settings, apart from 'Illegal Online Content', can be configured to the needs of the customer. Each of your SurfProtect profiles can be configured differently, allowing you to tailor settings to specific groups of users - younger and older students, teachers, safeguarding staff etc.

There are a number of questions that the UK Safer Internet Centre recommends asking your filtering provider to ensure the filtering system you are implementing is appropriate. Here, we'll highlight what you need to know about our SurfProtect products.

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

SurfProtect enables you to adjust the filtering strength by age, vulnerability and role through flexible profile settings.

You can create tailored policies for year groups, staff, departments, or individual users, ranging from tightly controlled “walled garden” access for younger pupils to broader access for older students and staff.

With Active Directory integration, filtering can be applied based on individual users or groups, ensuring users receive the appropriate level of protection wherever they log in. Profiles can also be linked to devices or network locations where needed.. Profile prioritisation ensures that if a user belongs to multiple groups, the most appropriate policy is always applied, making it easy to provide additional safeguards for vulnerable learners while maintaining suitable access for others.

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

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 where a blocked domain is embedded within another service (for example, via Google Translate). VPNs and proxy services are categorised under a dedicated “Proxies” category within SurfProtect, which is blocked by default.

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.

However, more advanced VPN technologies designed specifically to evade filtering may mask their traffic and not rely on standard ports or protocols. In these cases, additional measures are recommended to minimise the risk of circumvention e.g. stringent cyber security policies or device management controls to enforce expected configurations and restrict the installation or use of unauthorised applications.

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. To further prevent evasion, SurfProtect also restricts the use of Encrypted Client Hello (ECH) on filtered devices, ensuring that destination information cannot be concealed during TLS negotiation.

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 enables authorised staff to review and edit filtering policies at any time, from any location with an internet connection, ensuring schools retain full control over their filtering environment.

Through the portal, schools can easily allow or block specific websites, regardless of their category classification, giving them the flexibility to tailor filtering policies to their individual requirements. Changes are applied in real time, meaning access to appropriate resources can be granted immediately, and inappropriate content restricted without delay.

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

All actions taken within the portal are logged, providing a clear audit trail of changes to filtering settings. This ensures transparency and accountability, while supporting safeguarding and compliance requirements.

For Multi-Academy Trusts and managed service providers, SurfProtect also offers a hierarchical access model. This allows central teams to manage multiple schools from a single interface, while individual schools retain control over their own settings.

- 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, SurfProtect downloads and analyses the content to determine an accurate classification, before deciding whether to display the page according to your policies. Websites are then revisited on a regular basis to confirm their classification remains accurate as content changes over time.

Filtering decisions are made based on this classification approach, rather than real-time analysis of content as it is streamed to the user. However, due to the rapidly evolving and user-driven nature of Generative AI, SurfProtect applies a precautionary approach by blocking AI-related categories and keywords by default. Schools can choose to enable access where appropriate, in line with safeguarding policies and relevant guidance, ensuring they retain full control over how such content is accessed within their environment.

- 6. Can the filtering system be deployed in a variety and combination of ways (e.g. on device, network level, cloud, DNS)?**

SurfProtect is delivered as a cloud-based filtering solution, or using an on-premise device depending on your requirements. Deployment typically involves configuring a customer's network to route web traffic through SurfProtect, using a range of supported methods depending on the organisation's requirements.

In addition to network-level configuration, SurfProtect can also be deployed and managed through a combination of device-level approaches. Customers can enforce web proxy settings on devices to direct traffic to SurfProtect, with deployment commonly managed using tools such as Group Policy Objects (for Windows environments) or Mobile Device Management (MDM) solutions for other device types.

For environments using Active Directory, an AD proxy configuration can be implemented, enabling SurfProtect to associate user identities with web requests. Alternatively, customers can deploy a Proxy Auto-Configuration (PAC) file across devices, allowing traffic to be directed through SurfProtect via a centrally managed configuration.

These flexible deployment options allow it to be used effectively in a variety of combinations across network and device levels.

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

You can find SurfProtect's filtering policy on page 5 of this document.

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

As mentioned in question 4 SurfProtect offers a hierarchical access model. This allows central teams to manage multiple schools from a single interface, while individual schools retain control over their own settings. 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.

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.

9. Does the filtering system have the ability to identify users and devices to attribute access (particularly for mobile devices) and allow the application of appropriate configurations and restrictions for individual users?

SurfProtect provides multiple methods to associate web requests with individual users, enabling schools to apply appropriate filtering policies based on user identity.

Through Active Directory integration, SurfProtect can identify Windows users and attribute their web activity accordingly, allowing policies to be applied at a user or group level. SurfProtect Quantum+ also offers a Captive Portal solution which is suitable for school-managed devices, BYOD, and devices used off-site. This presents users with a login prompt where they can authenticate using their AD credentials, Google Workspace account, or Microsoft Entra account, enabling their activity to be linked to their identity.

SurfProtect's self-administration panel allows customers to create custom filtering profiles that can be associated with specific usernames or group names. These profiles are then automatically applied when matching user identity data is detected in web requests, ensuring that appropriate configurations and restrictions are enforced on a per-user basis across a range of device types, including mobile devices.

10. 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, intercepting and inspecting requests regardless of how they are generated. This approach makes the service agnostic to the source of the traffic, enabling it to apply filtering consistently across devices.

As long as content is delivered over standard web protocols (HTTP/HTTPS), SurfProtect is able to identify and enforce filtering policies in the same way, whether the request originates from a browser or an application. This ensures that inappropriate content accessed via mobile devices and apps is subject to the same controls and protections as typical web-based content, provided that traffic is routed through SurfProtect.

11. 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 Safe Search on all major search engines to ensure that inappropriate search terms cannot be entered in any language.

12. With many children and staff working remotely, to what ability do school owned devices to receive the same or equivalent filtering to that provided in school?

SurfProtect Quantum+'s PAC solution enables devices that are taken out of schools to be dynamically configured with a captive portal-enforcing proxy, enabling the filtering and association of web requests to users even when off the schools network.

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

Authorised users with access to the self-administration panel can directly manage their filtering settings, allowing them to permit or block specific content as required.

Customers can also report websites they believe to be incorrectly classified or requiring further review to the support team. This can be done via the HelpDesk or through the web chat functionality available on both the main website and within the self-administration panel.

14. 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.

SurfProtect Analytics enables schools to review detailed reports on browsing behaviour, supporting safeguarding and incident investigation requirements. Real-time alerting can be configured to notify nominated staff of specific types of blocked activity, ensuring that potential concerns can be identified and addressed promptly.

15. Does the filtering system have the ability to enforce 'safe search' when using search engines?

SurfProtect provides the ability to enforce 'Safe Search' and is enabled by default within SurfProtect. Where HTTPS decryption is in place, these settings are enforced directly through web traffic inspection.

In scenarios where HTTPS traffic is not decrypted, SurfProtect DNS supports this functionality by redirecting requests from well-known search engines to their safe search equivalents. This ensures that Safe Search protections remain in place regardless of deployment configuration, helping schools maintain a consistent level of safeguarding for users.

16. Does the filtering system have the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity

Historical and real-time analytics can be exported in CSV format, allowing schools to import this data into their chosen safeguarding or monitoring platforms. This enables wider analysis of user activity alongside other contextual information, helping schools to build a more complete picture of behaviour and identify potential concerns more effectively.

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 radicalisation.

How can SurfProtect® help?

SurfProtect® 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 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. 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.