**Filtering Advice**

Version 1.0

Contents

[1. What is Internet Filtering? 2](#_Toc76325703)

[2. Types of Filtering 2](#_Toc76325704)

[3. Filtering Requirements 3](#_Toc76325705)

[3.1 Block access to the IWL URL List 3](#_Toc76325706)

[3.2 Block access to the police assessed list of unlawful terrorist content 3](#_Toc76325707)

[4. Managed / Unmanaged Filtering 3](#_Toc76325708)

[4.1 Managed filtering solutions 3](#_Toc76325709)

[4.2 Unmanaged filtering solutions 3](#_Toc76325710)

[5. Complying with Legislation 4](#_Toc76325711)

[6. Test your Filtering 5](#_Toc76325712)

[7. Teaching and Reporting, rather than enforcing 5](#_Toc76325714)

[8. Reporting Inappropriate Content 6](#_Toc76325715)

[8.1 Suspicious behaviour towards a child 6](#_Toc76325716)

[8.2 Child sexual abuse images 6](#_Toc76325717)

[8.3 Online terrorism 6](#_Toc76325718)

[8.4 Hate Crime 6](#_Toc76325719)

[8.5 Cybercrime 6](#_Toc76325720)

# What is Internet Filtering?

Is important that schools provide access to the digital world but also ensure that children don’t stumble across inappropriate content isn’t just good practice, it is covered by law.

Internet filtering allows settings to control the sites which children can or can’t access. It is possible to block the most harmful content as well as specific sites, which can help to enforce school policies on social media content, for example.

Sometimes it is referred to as ‘content-control software’ or ‘web filtering’. It can be used to restrict or control access to internet sites and email.

# Types of Filtering

There are many different types of filtering:

* **Browser based filters** – typically via a browser extension.
* **Email filters** - mail filters look at headers such as sender, subject, email attachments, and the contents of the message to classify, accept, or reject messages.
* **Filtered ISPs** - Filtered ISPs are Internet service providers that provide access to only approved parts of the Internet.
* **Network-based filtering** – often implemented as a web-proxy. All users are subject to the access policy defined by the provider. The filtering can be customised, so pupils and staff can have different levels of filtering.
* **DNS-based filtering** – Prevents lookups for domains (sites) that do not fit a set of policies defined by the setting.
* **Search-engine filters** - Many search engines, such as Google and Bing offer users the option of turning on a safety filter. This only works on internet searches and not when pupils type in addresses.
* **Child-friendly search engines** - designed so only child-friendly websites are allowed.

Whilst you should be using internet filtering to safeguard and protect your pupils from accessing inappropriate content, you should also protect your systems and school community with basic security controls such as firewalls, and an anti-virus and anti-malware product which is regularly updated and monitored.

For more information on basic cyber security measures, refer to guidance from the National Cyber Security Centre (NCSC).

<https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools>

<https://www.ncsc.gov.uk/collection/10-steps>

# Filtering Requirements

* 1. Block access to the [IWF URL List](https://www.iwf.org.uk/become-a-member/services-for-members/url-list), previously called the Child Abuse Images and Content list (CAIC).

The [Internet Watch Foundation](https://www.iwf.org.uk/) (IWF) maintains a list of URLs for individual webpages with child sexual abuse content. Filtering solutions can incorporate the URL List to protect children from accidentally accessing these pages.

Search providers can also use the list to stop these pages from being indexed, so they don’t show up in search results.

If your provider isn’t meeting the requirements, they can contact the IWF via: [members@iwf.org.uk](mailto:members@iwf.org.uk) or call 01223 203030.

* 1. Block access to the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.

Refer to the [Prevent Duty Toolkit](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/736759/Prevent_Duty_Toolkit_for_Local_Authorities.pdf) (Home Office).

The Department for Education has set up a helpline for teachers who have questions and/or concerns about extremism.

Teachers can call: [0207 340 7264](tel:02073407264)or email: [counter.extremism@education.gov.uk](mailto:counter.extremism@education.gov.uk) for support.

# Managed / Unmanaged Filtering

4.1 A managed filtering solution is controlled by your provider. It is most suited to those with little technical support on site.

The advantages are that you pay the provider to ensure that the filtering is ‘fit for purpose,’ and meets the requirements as set out in your contract. It is the most ‘hassle-free’ option.

The disadvantage is that you have less control, and may find sites you would like access to, blocked. Whilst you can make a request to the provider, you may find the service restricts the change.

4.2 An unmanaged filtering solution is controlled by your organisation. It is most suitable for those with on-site technical support or a proactive off-site technician.

The advantages are that you have the most flexibility and can tailor the solution to suit your requirements. It can be faster to make adjustments, which is useful when lesson plans change.

The disadvantages are that fine-tuning filtering can take time and may leave gaps / vulnerabilities, and if there is a change of technical staff it can be difficult to determine the current status of the filtering product.

# Complying with Legislation

You are required by law “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering”. This is laid out in The Prevent Duty, part of the Counter-Terrorism and Security Act 2015.

Refer to both the Home Office’s [Prevent Duty](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty) and the [Revised Prevent Duty Guidance: England and Wales](https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales)

*IT Policies*[[1]](#footnote-1)

*“The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.*” [Schools in England (and Wales)]

The Department for Education’s statutory guidance ‘[Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)’ (KCSIE) (point 95) obliges schools and colleges in England to “ensure appropriate filters and appropriate monitoring systems are in place”

*Protecting Children*[[2]](#footnote-2)

*“Governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the above risks from the school’s or college’s IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place.”*

In 2013 Ofsted released the first e-safety inspection framework and concluded that pupils attending settings with managed systems had a better knowledge and understanding of how to stay safe, than those in schools with ‘locked down’ systems.

The e-safety inspection framework was incorporated into the Common Inspection Framework which refers to the need for filtering. In the [Inspecting safeguarding in early years, education and skills settings](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/828763/Inspecting_safeguarding_in_early_years__education_and_skills.pdf) guidance for inspectors it states:

[*Inspecting how effectively leaders and governors create a safeguarding culture in the setting*](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/828763/Inspecting_safeguarding_in_early_years__education_and_skills.pdf)[[3]](#footnote-3)

*“ - appropriate filters and monitoring systems are in place to protect learners from potentially harmful online material.”*

Ofsted has noted that settings with locked down systems gave pupils fewer opportunities to learn how to assess and manage risk for themselves. Strict filtering also significantly impacts useability and functionality. This had been supported by a very small-scale study in 2009.[[4]](#footnote-4)

# Test your Filtering

The [SWGfL](https://swgfl.org.uk/) (South West Grid for Learning) have a free tool to support schools in evaluating their filtering.

Go to: <http://testfiltering.com/schools>



**Click**

You do not have to provide organisational details to use the filter test, but do ensure that you have selected ‘school’.



****

**Click**

You will receive a message with: **Results for Filter Test:** Failed  **or** Passed

# Teaching and Reporting, rather than enforcing

The proposed [Online Safety Bill](https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published) is designed to protect young people and clamp down on racist abuse online, while safeguarding freedom of expression. The bill provides a legal framework for identifying, reporting, and removing harmful content.

The legislation supports online safety, but no legislation can guarantee the internet as safe. Equally, no filtering system makes the internet completely safe all of the time. Filtering is often a ‘best fit’ of usability and safety.

It is important young people understand the risks and potential dangers of the online world and learn to make safe decisions. It is vital **all** users understand appropriate online behaviour, supported by robust policy, clear guidance, and relevant training.

Over-restricting access can be counterproductive. Just as we teach children to swim and cross the road safely, we must teach them to make safe decisions online, where possible. Make sure your school teaches pupils who and where to go to for help when they are in doubt, and report anything they see which concerns or worries them.

Online safety can be taught in an age appropriate way from nursery age and needs to continue as teens navigate the digital world into adulthood.

Ensure that your online safety curriculum is inclusive and differentiated to enable learners with SEND to access the internet safely and appropriately.

# Reporting Inappropriate Content

* 1. Suspicious behaviour towards a childshould be reported to the CEOP, the [Child Exploitation Online Protection Centre.](https://www.ceop.police.uk/ceop-reporting/)

In an emergency, contact the emergency services by calling 999.



Child Exploitation and Online Protection Command **(CEOP)** is a command of the National Crime Agency, a law enforcement agency which works to pursue and prosecute child sex offenders.

**CEOP** works with child protection partners across the UK and overseas to identify the main threats to children, and coordinates activity against these threats to bring offenders to account.

****

8.2 Child sexual abuse imagesshould be reported to the Internet Watch Foundation  [www.iwf.org.uk/report](http://www.iwf.org.uk/report)

8.3 Online terrorism content should be reported to the police’s **Counter Terrorism Internet Referral Unit** at[www.gov.uk/report-terrorism](http://www.gov.uk/report-terrorism)



8.4 Hate Crime, victimisation on the grounds of race, religion, disability, sexual orientation or gender should be reported to **True Vision** at [www.report-it.org.uk](http://www.report-it.org.uk)



8.5 Cybercrime, including phishing, scams, fraud, and suspicious activity should be reported to report **Action Fraud** 24/7 on **0300 1232040** or [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

1. [The Prevent Duty](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf) – departmental advice p8 [↑](#footnote-ref-1)
2. [KCSIE](Keeping%20Children%20Safe%20in%20Education) Protecting Children p103 [↑](#footnote-ref-2)
3. [Inspecting safeguarding in early years, education and skills settings](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/828763/Inspecting_safeguarding_in_early_years__education_and_skills.pdf) p14 [↑](#footnote-ref-3)
4. [Ofsted – Safe Use of Technologies](https://webarchive.nationalarchives.gov.uk/20141107033803/http:/www.ofsted.gov.uk/resources/safe-use-of-new-technologies) [↑](#footnote-ref-4)