Appropriate Filtering for Education settings

xxx 2026

Schools[1] in England (and Wales) are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*"[2]. Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' [3] obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks*[4] *from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*." Ofsted concluded as far back as 2010[5] that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves."

To further support schools and colleges in England to meet digital and technology standards, the Department for Education published Filtering and Monitoring Standards[6] in March 2023 (as part of a broader suite of educational technology standards and guidance)[7]. In addition to aspects of both filtering and monitoring systems, these standards detail the allocation of roles and responsibilities, and that schools and colleges should be checking their filtering and monitoring provision at least annually. These standards were included within Keeping Children Safe in Education in 2023.

The Welsh Government has published a common set of agreed standards for internet access provides the tools for schools to make informed choices over filtered provision whether delivered by the local authority or another provider[8].

Previously included within the Scottish Government national action plan on internet safety [9], schools in Scotland are expected to "*have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content*."

---

[1] The schools and registered childcare settings specified in Schedule 6 of the Counter-Terrorism and Security Act 2015 (CTSA 2015)

[2] Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/publications/prevent-duty-guidance

[3] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

[4] Keeping Children Safe in Education Paragraph 136, Page 35 – Content, Contact, Conduct, Commerce

[5] Safe Use of New Technologies - http://webarchive.nationalarchives.gov.uk/20141107033803/http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies

[6] https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

[7] Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK (www.gov.uk)

[8] Web Filtering Standards - Hwb (gov.wales) https://hwb.gov.wales/support-centre/education-digital-standards/web-filtering-standards

[9] National Action Plan on Internet Safety for Children and Young People, April 2017, http://www.gov.scot/Publications/2017/04/1061

The aim of this document is to help education settings (including Early years, schools and FE) and filtering providers comprehend what should be considered as 'appropriate filtering'.

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision. As such, filtering systems should be recognised as one of the tools used to support and inform the broader safeguarding provision in settings.

Illegal Online Content

The Online Safety Act now sets out[10] the kinds of illegal content and activity that includes content relating to:

child sexual abuse	Content that depicts or promotes sexual abuse or exploitation of children, which is strictly prohibited and subject to severe legal penalties.
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts.
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.
extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.
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.
inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.
illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.
intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.
selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.
terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.

Schools should satisfy themselves that their filtering system manages this type of content specifically that the filtering providers:

- Are IWF members and use IWF services to block access to illegal Child Sexual Abuse Material (CSAM)
- Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

[10] Online Safety Act: explainer - GOV.UK

Schools and colleges must make sure these blocklists are implemented within 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 (LA) or any other responsible body, including system administrators, at any level. [Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, schools should be satisfied that their filtering system additionally manages the following inappropriate content (and web search) including 'Primary Priority Content' and 'Priority Content' (as described by the Online Safety Act)

Content	Explanatory notes – Content that:
Gambling	Enables gambling
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
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.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content, including ransomware and viruses
Mis / Dis Information	Promotes or spreads false or misleading information intended to deceive, manipulate, or harm, including content undermining trust in factual information or institutions
Piracy and copyright theft	includes illegal provision of copyrighted material
Pornography	displays sexual acts or explicit images and text
Self-Harm and eating disorders	content that encourages, promotes, or provides instructions for self-harm, eating disorders or suicide
Violence Against Women and Girls (VAWG)	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.

This list should not be considered an exhaustive list, and providers will be able to demonstrate how their system manages this content and many other aspects.

Regarding the retention of logfile (Internet history), as the data controller, schools should understand their filtering providers data retention policies including the duration to which all data is retained and have associated data sharing agreements. Logfiles (Internet history) should include the identification of individuals and/or devices.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions. Welsh Government highlight that "It is critical that filtering standards are fit for purpose for 21*st* century teaching and learning, allowing the access schools require whilst still safeguarding children and young people."[11]

[11] Welsh Government Filtering Standards https://hwb.gov.wales/support-centre/education-digital-standards/web-filtering-standards#document

Given the extent of personal data involved with some filtering systems, Schools and Colleges should consider undertaking a Data Protection Impact Assessment[12] and ensure that this aligns with the organisational policies.

Filtering System Features

Additionally, and in context of their safeguarding needs, schools should consider the required features of their filtering system;

- Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff
- Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services, DNS over HTTPS and ECH.
- Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes.
- Contextual Content Filters –
  Contextual content filtering refers to the ability to analyse online content based on its meaning and context, rather than relying solely on website categories or domain lists. Appropriate filtering systems should be capable of identifying harmful or inappropriate content within otherwise permitted platforms, including dynamically generated webpage content.
  As most online traffic is encrypted, schools and colleges should understand how their filtering system analyses encrypted connections and whether contextual inspection takes place on decrypted content. Filtering providers should be transparent about how encrypted traffic is handled and any technical limitations that affect the system's ability to analyse content in real time, so that schools can make informed safeguarding decisions.
- Deployment – filtering systems can be deployed in a variety (and combination) of ways (e.g. on device, network level, cloud, DNS). Providers should describe how their systems are deployed alongside any required configurations and/or limitations. As technology and security standards evolve, relying solely on network-level filters may become increasingly challenging and less effective. Schools might consider combining network-level filtering with device-level configurations tailored to school-owned and managed devices.
- Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as how the system addresses over blocking
- Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard
- Identification - the filtering system should 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. This would ensure safer and more personalised filtering experiences.
- Mobile and App content –
- Filtering should apply to content accessed through mobile devices and applications, as well as traditional web browsing. This includes content viewed, uploaded, or processed by apps used on school or college devices, including where apps request access to cameras, microphones, photo libraries, file storage, or cloud services.
  Schools and colleges should understand that some app functionality relies on user-granted permissions and cloud or device-side processing, which may limit the extent to which filtering can

[12] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

intervene once access has been permitted. Filtering providers should clearly explain what filtering is technically possible across different device types and operating systems, and any limitations that apply, so that schools can take these into account within their wider safeguarding arrangements.

- Multiple language support – the ability for the system to manage relevant languages
- Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school
- Reporting mechanism – the ability to report inappropriate content for access or blocking
- Reports – the system offers clear granular historical information on the websites users have accessed or attempted to access
- Safe Search – the ability to enforce 'safe search' when using search engines
- Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity

Schools and Colleges should ensure that there is sufficient capability and capacity in those responsible for, and those managing, the filtering system (including any external support provider). The UK Safer Internet Centre Helpline[13] may be a source of support for schools looking for further advice in this regard.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum"*[14]. To assist schools and colleges in shaping an effective curriculum, UK Safer Internet Centre has published ProjectEVOLVE[15]

Risk Assessment

UK Safer Internet Centre recommends that those responsible for Schools and Colleges undertake (and document) an online safety risk assessment at least annually or whenever any substantive changes occur, assessing their online safety provision that would include filtering (and monitoring) provision. The risk assessment should consider the risks that both children[16] and staff may encounter online, together with associated mitigating actions and activities.

A risk assessment module has been integrated in *360 degree safe*[17]. Here schools can consider identify and record the risks posed by technology and the internet to their school, children, staff and parents.

Checks and Documentation

Schools and Colleges should regularly check that their filtering and monitoring systems are effective and applied to all devices. Checks should be conducted when significant changes take place (for example, technology, policy or legislation), in response to incidents and at least annually. These checks should be recorded, including details about the location, device and user alongside the result and any associated action.

SWGfL testfiltering.com enables users to test fundamental capabilities of their filtering system and to inform improvement.

---

[13] https://www.saferinternet.org.uk/helpline
[14] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
[15] ProjectEVOLVE - Education for a Connected World Resources (https://projectevolve.co.uk/)
[16] http://netchildrengomobile.eu/ncgm/wp-content/uploads/2014/11/EU-Kids-Online-Net-Children-Go-Mobile-comparative-report.pdf
[17] www.360safe.org.uk, https://360safecymru.org.uk/, http://www.360safescotland.org.uk/

Filtering on Mobile devices

Schools and colleges should satisfy themselves that filtering systems are correctly working across all their devices' and across all internet connections, including their mobile devices. If your school owns mobile devices such as iPads or other tablets as part of your teaching strategy, then consider the following practices to ensure filtering is in place (you may need the help of your ICT support to do this):

For schools and colleges in England, the following DfE guidance is relevant

- Digital leadership and governance standards - Guidance - GOV.UK (www.gov.uk) – specifically guidance related asset registers in context of points 1 and 2 below
- Laptop, desktop and tablet standards - Guidance - GOV.UK (www.gov.uk)
- Mobile phones in schools - GOV.UK (www.gov.uk)

1. Audit the mobile device estate by detailing all the mobile devices they have.
2. Understand and detail the applications (apps) they use and how these are managed (installed and deleted). Specifically, ensure that apps can be centrally, and routinely, removed from mobile devices. This is best achieved through the use of a Mobile Device Management (MDM). Where apps include embedded browsers or open links in other apps, schools and colleges should confirm whether monitoring (and reporting) applies to that activity
3. Identify who is responsible for mobile devices as well as filtering and monitoring solutions at the school, ensuring that the DSL is also aware (if different).
4. Test to provide confidence that the school's filtering and monitoring solution is working across all mobile devices, across installed apps (not just internet browsers) and in various physical locations. Schools can use testfiltering.com to help observe filtering behaviour on their connection, including where additional configuration (for example managed devices, certificates, or managed browsers) is required for particular tests.
5. Identify any vulnerable users of mobile devices, paying particular attention to ensure harmful content is not accessible on specific devices

Generative AI Technologies

New technology is enabling users to generate personalised content in real-time based on prompts and schools are being encouraged to exploit these potential advantages for "faster planning and record-keeping"[18]. The real-time nature and proliferation of these system present a challenge to schools when it comes to filtering this type of content. Filtering systems should effectively and reliably prevent access to harmful and inappropriate content generated by Generative AI systems. Schools should reflect on the following, as part of any risk assessment, when considering their systems and deciding what generative AI systems they allow students and staff to use:

- The level to which your filtering system can block content in real-time
- Assessing which generative AI systems the school which to approve for use after assessing safety features, and data protection
- Developing a policy around the use of generative AI systems
- Assessment of your ability to generate reports on the usage or generative AI systems within school

Further Governmental considerations for adopting Generative AI technologies in schools:

[18] Artificial Intelligence: Plan to 'unleash AI' across UK revealed - BBC News

- England – Generative artificial intelligence (AI) in education - GOV.UK (Jan 2025)

  The DfE's *Generative AI: Product Safety Expectations* sets out clear guidance for ensuring AI tools used in schools are safe by design, including expectations for risk assessment, content moderation, transparency, and reporting—providing a helpful benchmark when determining which generative AI platforms should be accessible through school filtering systems.

- Wales - Generative artificial intelligence in education - Hwb (Jan 2025)

This detail has been developed by the SWGfL, as a partner of the UK Safer Internet Centre, and in partnership and consultation with the 80 national '*360 degree safe Online Safety Mark*'[19] assessors and the NEN Safeguarding group (www.nen.gov.uk).

[19] www.360safe.org.uk, https://360safecymru.org.uk/, http://www.360safescotland.org.uk/