Appropriate Filtering for Education settings

UK Safer Internet Centre
www.saferinternet.org.uk
brought to you by SWGfL Childnet International IWF

June 2021

Schools 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*”[1]. Furthermore, the Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ [2] obliges schools and colleges in England to “*ensure appropriate filters and appropriate monitoring systems are in place” and they “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*” 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 in 2010[3] 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.”

Included within the Scottish Government national action plan on internet safety[4], 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*.”

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.

Illegal Online Content

In considering filtering providers or systems, schools should ensure that access to illegal content is blocked, specifically that the filtering providers:

- Are IWF members and 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’

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

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

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

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

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, schools should be satisfied that their filtering system manages the following content (and web search)

Content	Explanatory notes – Content that:
Discrimination	Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
Pornography	displays sexual acts or explicit images
Piracy and copyright theft	includes illegal provision of copyrighted material
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)
Violence	displays or promotes the use of physical force intended to hurt or kill

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), schools should ensure clear and appropriate data retention policies and logfiles (Internet history) should include the identification of individuals and the duration to which all data is retained.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions.

Filtering System Features

Additionally, and in context of their safeguarding needs, schools should consider how their filtering system meets the following principles

- Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role
- Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services and DNS over HTTPS
- Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content
- Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked. For example, being able to contextually analyse text on a page and dynamically filter.
- Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as 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
- Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)
- Multiple language support – the ability for the system to manage relevant languages

- Network level - filtering should be applied at 'network level' i.e., not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)
- Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school
- Reporting mechanism – the ability to report inappropriate content for access or blocking
- Reports – the system offers clear historical information on the websites visited by your users

Schools and Colleges should ensure that there is sufficient capability and capacity in those responsible for and those managing the filtering system. The UK Safer Internet Centre Helpline[5] 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*"[6]. To assist schools and colleges in shaping an effective curriculum, UK Safer Internet Centre has published ProjectEVOLVE[7]

UK Safer Internet Centre recommends that those responsible for Schools and Colleges undertake (and document) an annual online safety risk assessment, assessing their online safety provision that would include filtering (and monitoring) provision. The risk assessment should consider the risks that both children[8] and staff may encounter online, together with associated mitigating actions and activities.

A risk assessment module has been integrated in *360 degree safe*[9]. Here schools can consider identify and record the risks posed by technology and the internet to their school, children, staff and parents.

To improve the appreciation of filtering services, SWGfL developed an online utility that enables users to discover capabilities of their filtering system.

[5] https://www.saferinternet.org.uk/helpline

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

[7] ProjectEVOLVE - Education for a Connected World Resources (https://projectevolve.co.uk/)

[8] http://netchildrengomobile.eu/ncgm/wp-content/uploads/2014/11/EU-Kids-Online-Net-Children-Go-Mobile-comparative-report.pdf

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

This detail has been developed by the SWGfL, as a partner of the UK Safer Internet Centre, and in partnership and consultation with the 120 national '*360 degree safe Online Safety Mark*'[10] assessors and the NEN Safeguarding group (www.nen.gov.uk).

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