Appropriate Filtering for Education settings

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 published the revised statutory guidance 'Keeping Children Safe in Education' [2]in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated to "*ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges 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*."

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 Abuse Images and Content (CAIC)
- Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

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 on the grounds of race, religion, age, or sex.
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

[1] Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

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

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.

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

Filtering System Features

Additionally schools should consider that their filtering system meets the following principles

- Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role
- Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content
- Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking
- Identification - the filtering system should have the ability to identify users
- Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies
- 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
- 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

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".*[3]

This detail has been developed by the South West Grid for Learning, as coordinators of the UK Safer Internet Centre, and in partnership and consultation with the 120 national '*360 degree safe e Safety Mark*' assessors (www.360safe.org.uk) and the NEN Safeguarding group (www.nen.gov.uk).

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