Appropriate Filtering for Education settings

September 2019

Filtering Provider Checklist Responses

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". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England 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"

Included within the Scottish Government national action plan on internet safety, 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."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

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.

Company / Organisation	E2BN
Address	Unit 1, Saltmore Farm, New Inn Road, Hinxworth, Herts, SG7 5EZ
Contact details	Philip Pearce
Filtering System	E2BNProtex
Date of assessment	10/01/2020

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

.

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
• Are IWF members		E2BN and E2BN Protex have been members of the IWF for 12 years. As active members of the IWF, we attending the funding council and help shape the IWF's work. (IWF – The Internet Watch Foundation – an organisation that finds and takes down child abuse materials as well as providing advice to central government.)
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		E2BN Protex blocks access to Child Abuse Images by actively implementing the CAIC list. The list is update twice a day and distributed to all E2BN Protex systems overnight. The list is hidden from all Protex users (including system administrators) and cannot be overridden.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		E2BN Protex implements the latest Home Office counter terrorist list as part of our support for 'PREVENT'. The list is hidden from all users (including system administrators) and cannot be overridden.

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		E2BN Protex filters discriminatory content through its 'intolerance' category which includes both URLs and Phrases for content checking. E2BN Protex filters all web-page requests against lists of known

			URLs as well as checking the page's content. Content checking – if a page is not blocked by its URL the default is to check its content by comparing it against our phraselists: the HTML of the page is scanned for a variety of phrases and patterns. There are two types of phrases: those which are banned and those that are weighted. A web page containing a word or phrase from the banned list is blocked. All words and phrases on a web page are compared to the weighted phraselist. The value of the words and phrases found on a page are totalled to give the page a numerical rating. We call this rating a 'naughtiness' value. Each profile has a 'naughtiness' threshold set to reflect the age group of the profile. If a page exceeds the 'naughtiness threshold' for the user's profile the page is blocked.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		E2BN Protex filters illegal drug use and substance abuse through its 'Drugs' category using the methods described above.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		E2BN Protex filters extremist content through its 'Extremism and 'Violence' categories using the methods described above.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		E2BN Protex filters malware and hacking sites through its 'File Hosting', 'Illegal Hacking' and 'Proxy' categories using the methods described above.

Pornography	displays sexual acts or explicit images		E2BN Protex filters pornography and other explicit sexual content through its 'Pornography' and 'Violence' categories using the methods described above. (Illegal sexual content is blocked via the IWF list mentioned above)
Piracy and copyright theft	includes illegal provision of copyrighted material		E2BN Protex filters content against the PIPCU (Police Intellectual Property Crime Unit) list provided by the Metropolitan Police.
Self-Harm	promotes or displays deliberate self-harm (including suicide and eating disorders)		E2BN Protex filters 'self-harm', 'pro-an', suicide and other pages depicting or promoting self-harm are through its 'Adult' category using the methods described above. This categorisation means that the pages are available via the Staff profile in order to allow school Staff to access these sites for research purposes or through guided whole class teaching in PSHE
Violence	Displays or promotes the use of physical force intended to hurt or kill		E2BN Protex filters violent content through its 'Violence' category using the methods described above.

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Additional Content Management

- There are various other categories of content checking and URL lists for other content. For example, “onlinegames” and “kidstimewasting” are generally blocked to students but not staff.

- For specific installations this default may be modified. For example, a Library may not want “onlinegames” blocked.

- A school’s Protex system administrators may exert more control over the way these categories are applied to their own users if they wish(i.e. they can create school specific profiles for particular groups of users applied via integration with, for example, their Active Directory)

- A school’s Protex system administrators (either school staff or as a service delegated to E2BN Protex) can modify the filtering by adding specific URLs to the set of Local Lists available on each Protex installation.

- E2BN Protex provides training and support for schools wishing to manage their own filtering categories and profiles.

- Alternatively they can apply any of the age-appropriate defaults profiles we supply.

- Application of the “Porn”, “illegalDrugs”, “illegalHacking” and “Proxy” categories cannot be overridden.

Use of search engines – Protex scans the submitted search and blocks unsuitable search terms as well as content checking the results page of each search

Image searches - Image searching is a very powerful tool but some schools have had to ban it because of the nature of some of the thumbnail images displayed to the unwary. E2BN Protex addresses this problem in two ways. Firstly safe search is enforced for all pupil filtering profiles when common search engine are accessed. However, even safe search is not fool proof. So, in addition, our system tests the URL of the originating site of each image returned. If Protex finds that it is a site which would be blocked to this user then the returned image is replaced with a blank one. Clearly, if the user clicks on the blank to go to the site it is blocked by the URL filter.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy.

End User Data

- E2BN does not retain logs of end users or their internet activity.
- Logfiles are stored on the school’s Protex box.
- For the purpose of The Data Protection Act and GDPR this data is the school’s responsibility.
- The log files are typically stored for a period of 6 to 9 months then older logs are overwritten as new logfiles are generated.

System Admin (self-managed systems)

Protex admins’ username and email address along with a record of every change made to the local URL lists and profiles, are held on the school’s Protex box and E2BN’s central control server. E2BN retains this data for 20 years for safeguarding, auditing and technical reasons.

When a school admin is deleted from the school's Protex box, the username and email details are automatically deleted from the E2BN central system. However, the log of changes to whitelists and profiles made by the school admin is maintained.

Centrally Managed Systems
All web requests for changes to local URL lists, profiles and blocking require the person making the request to provide a school email address. This information is retained by E2BN for safeguarding, auditing and technical reasons.

All changes made by a school's Protex admin are logged on the school's Protex box and backed up to E2BN central system.

Data is held for 20 years

E2BN technical staff (all holders of enhanced DBS certificates and trained on GDPR and Data Protection) can only access user logfile data for the purpose of technical support.

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

Over-blocking
We have various feedback mechanisms in place to avoid over blocking.

Each blocked URL generates a page displayed to the user. This page's wording and the information returned is age related. This page includes the option for the user (or their teacher) to fill in a simple form with a request for the page to be unblocked. These requests are centrally reviewed by authorised E2BN DBS cleared personnel. Changes are made (or not) as appropriate. Where the user has provided an email address the user is notified of the change.

Sites/URL/Pages that belong to a blocked category or reach the 'naughtiness' threshold for a profile can be accessed by adding them to a "whitelist". Schools that opt for self-management can whitelist sites/pages. We will whitelist sites/pages on behalf of schools that have opted for us to manage their filtering. Whitelisting requests can be made from the blocked page (see above) or by contacting the E2BN office.

Block request
An online form is used to make requests for pages to be blocked. Again these are centrally managed with an emailed reply on the action taken.

An emergency block request can also be made phoning the E2BN office.

There is a dedicated email address for all other filtering queries.

When changes are made locally by a self-managed school or requested by a centrally managed school, we assess the change and consider if it is a change that we should "adopt" and distribute across all Protex systems. For example, an individual school may discover an unblocked games site add it to the 'onlinegames' category. A member of our team will be notified to the change, assess the site and, if it meets the criteria for a non-educational game, add it to the central Protex

‘onlinegames’ category. Once changed centrally all Protex systems will be updated within about 15 minutes.

Safeguarding
Changes made by a system administrator (either School or E2BN staff) are logged centrally for audit, monitoring and review purposes. We can provide details of the changes made by local system administrators upon request.

Filtering System Features

How does the filtering system meet the following principles?

Principle	Rating	Explanation
● Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		Central System - The centralised system uses multiple age-related filter settings or profiles, each tailored to the specified age-group including one for Adults/Staff. The profiles available include: Primary, Middle, Secondary, 6th Form, and Staff. Each of the pupil profiles is available with or without access to ‘social’ sites such as Facebook, YouTube and Twitter and with or without access to games sites Schools that opt for self-management can apply our default profiles and customise the strength of the filter for groups, classes and even individuals. All schools can whitelist sites and pages from otherwise blocked categories (except where the site or page is listed on the IWF, Home Office or PIPCU lists or is categorised as ’illegal hacking’, ‘Pornography’, ‘Illegal Drugs’, or ‘Proxy’. Similarly schools can request the blocking of particular sites or pages.
● Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.		E2BN Protex subscribes to various commercial lists that list Proxy IPs, VPN application URLs and conducts its own audits into web filtering avoidance services that are being accessed and blocks these for all users. New methods continue to be blocked as they become apparent. With the Protex Pro service (which includes a firewall as well as web filtering) ports that may be used in an

		attempt to bypass the web filtering can be blocked at the firewall level.
● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Schools can modify the lists and create specific collections of list categories for their users via a simple to use web-interface (except where the site or page is listed on the IWF, Home Office or PIPCU lists or is categorised as 'Illegal Hacking', 'Pornography', 'Illegal Drugs', or 'Proxy'). The administration portal is accessible anytime, anywhere via the web interface.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		E2BN Protex provides details of its policy and approaches to filtering on the website. These policies have been developed in conjunction with users and local authorities over the past 12 years. The E2BN Protex filtering policy can be seen at: http://protex.e2bn.org/cms/policy.html
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Protex is a managed filtering service with centralised policy management specifically designed for schools. Schools can opt for central management or self-management. Multi-site management from a single interface is available. As a managed service, we also will make changes across any groups of schools on request.
● Identification - the filtering system should have the ability to identify users		Protex systems log the user associated with every request in two ways. Where Active Directory has been implemented on the schools system, all activity is logged against the users AD identity. On schools systems where AD integration is not desirable or possible users can be identified by IP Address if the school has a suitable identification system in place. A development, shortly to be released, will make it possible to insert the user's identity in the logs without using AD integration.
• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a		E2BN Protex is device agnostic: any device making requests using standard web protocols (including http and https) and

traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)		being directed to the Protex filtering server will be filtered. NOTE: Applications using proprietary protocols and/or proprietary encryption methods cannot be content filtered by this or any other filtering engine. Devices must be accessing content via the school network. Content such as phones and BYOD accessing the Internet via the device's 3G or 4G service cannot be filtered.
● Multiple language support – the ability for the system to manage relevant languages		The Protex filtering engine itself can handle any well formatted URL and content checking in multiple languages. Currently Protex supports content checking of English language text with some support for foreign languages.
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		Yes. All web-traffic is filtered when directed via the Protex filters. No client software is required.
● Reporting mechanism – the ability to report inappropriate content for access or blocking		Centralised system users complete our online forms to report sites that are not blocked and to make requests for blocked sites to be unblocked. Users can also report sites for an 'emergency' block by telephone during office hours. Local system users manage blocking and unblocking via the system admin interface in line with the school's own policies and procedures. All such changes are logged centrally providing a complete record of who, when and what changes are made.
● Reports – the system offers clear historical information on the websites visited by your users		All web requests, search terms and page visits are logged by user and time stamped. The system produces a range of standard reports on activity – for example for the most visited sites, most blocked categories, most blocked user/ group, most frequent search terms, activity by user or group etc. Additional bespoke reports can also be produced. All access to the admin interface is logged. Logs are typically held for between 6 & 9 months depending on volume.

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".*[1]

Please note below opportunities to support schools (and other settings) in this regard

Please note below opportunities to support schools (and other settings) in this regard E2BN offer e-safety training for staff and parents. E2BN has an area its website dedicated to e-safety (https://www.e2bn.org/cms/e-safety/e-safety)

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

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Philip Pearce
Position	Strategic Technical Manager
Date	10/01/2020
Signature