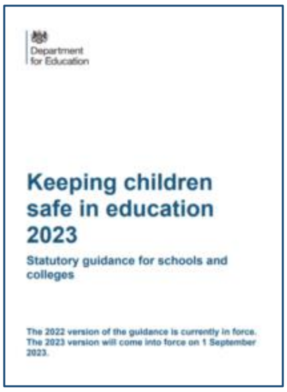
Integra is the trading arm of South Gloucestershire Council

integra. schools

IT Filtering and Monitoring Systems



Department for Education

Keeping children safe in education 2023

Statutory guidance for schools and colleges

The 2022 version of the guidance is currently in force. The 2023 version will come into force on 1 September 2023.

An updated version of Keeping Children Safe in Education (KCSiE) comes into force on the 1 September 2023. The updates include a new *emphasis on IT filtering and monitoring systems with a role for governing boards in making sure standards are met in this area.*

Integra, Schools IT have provided the following answers for schools who subscribe to their Broadband service.

1. Is your filtering provider:

a. A member of Internet Watch Foundation (IWF)?
Yes, the company we use that provides the filtering platform is a member of the IWF.

b. Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)?
Yes, the company provides a specific filtering category that contains this list.

c. Blocking access to illegal content including child sexual abuse material (CSAM)?
Yes, we use the categories provided by the filtering provider to ensure content is blocked.

In addition to the above, we use a separate reporting system that notifies us within 60 seconds if anyone on the network attempts to access any content on these lists.

2. Is the school's filtering operational and applied to all:

a. Users, including guest accounts?
Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to.

b. School owned devices?
Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to.

c. Devices using the school broadband connection?
Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to.

3. Does the filtering system:

a. Filter all internet feeds, including any backup connections?
Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to. All connections implemented or managed by Integra IT are subject to the filtering.

b. Be age and ability appropriate for the users, and be suitable for educational settings?
Yes, we utilise authentication to age-appropriate filtering. By default (with no authentication provided) the applied filtering levels are the most restrictive while being appropriate for the youngest users of the network.

c. Handle multilingual web content, images, common misspellings and abbreviations?
The filtering system is capable of handling all character sets (languages). It does not scan the content of images. Misspellings are included within the categories and can also be added manually.

d. Identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them?
Yes, we are able to block based on category and application type, we have automated/dynamic application filters that automatically block all known and new/emerging bypass technologies (VPNs, Proxy servers, etc…) for all users/devices on the network.

e. Provide alerts when any web content has been blocked?
Yes, all network & internet use is logged. All attempts to access blocked content or blocked applications or bypass attempts raise alerts. In addition to these we also block applications that are not deemed appropriate for use on the network, some of these applications (facebook, Instagram, twitter, etc…) are tied into many websites that are used everyday by schools, we do not generate alerts on these blocks as they are expected to occur.

4. Has the provider confirmed that filtering is being applied to mobile and app content?

Apps use many different methods to display their content. Some we are able to filter and others we cannot.

By default though, we block (in their entirety) mobile apps that are not specifically requested by schools.

5. Has a technical monitoring system been applied to devices using mobile or app content?

Schools can add additional monitoring to these devices if they wish.

6. Does the filtering system identify:

a. Device name or ID, IP address, and where possible, the individual?
Yes

b. The time and date of attempted access?
Yes

c. The search term or content being blocked?
Yes

7. Are there any additional levels of protection for users on top of the filtering service, for example, SafeSearch or a child-friendly search engine?

Yes, we enforce network wide SafeSearch (for all users) and restrict access to only search engines that fully support SafeSearch. This includes some mediated and/or child specific search engines, e.g. kiddle.co, kidrex.org, kidzsearch.com, safesearchkids.com, swiggle.org.uk, etc…

Kiddle.co and kidzsearch.com are very good at providing safe image searches too!

8. Does the monitoring system review user activity on school and college devices effectively? (For example, does it pick up incidents urgently, through alerts or observations, allowing prompt action to be taken; and is the response recorded)?

Yes, the monitoring system generates an alert within 60 seconds. Currently these alerts are sent to 3rd line IT staff for investigation. If the alert requires a response from school, a service ticket is generated and sent to the DSL for the school.

We believe we have been able to tune most false positives out of the system, so our intention is to have these alerts raised directly to the DSL for investigation in the near future. It will never be possible to accurately remove all false positives from the system, but they have been sufficiently reduced to minimise unnecessary alert emails.

9. Does the monitoring system ensure that incidents, whether of a malicious, technical, or safeguarding nature are picked up urgently?

The system generates the alerts as quickly as possible within 60 seconds. This ensures the relevant staff are aware that an incident needs to be investigated.