Appropriate Monitoring for Schools

May 2023

Monitoring Provider Checklist Responses

Schools (and registered childcare providers) 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, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

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 and regularly review their effectiveness" and they* "*should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] 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*."

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

The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is 'appropriate' for them.

Company / Organisation	Securly
Address	Third Floor One London Square, Cross Lanes, Guildford, Surrey, United Kingdom, GU1 1UN https://www.securly.com/
Contact details	uksales@securly.com 0141 343 8322
Monitoring System	Securly Filter, Aware and On-call
Date of assessment	3rd August 2023

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.	🟨

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
● Are IWF members	🟩	Securly has been an IWF member since 01/03/2016
● Utilisation of IWF URL list for the attempted access of known child abuse images	🟩	Securly receives and incorporates the IWF and CTIRU feeds into its filtering technology Securly blocks access to illegal content including CSAM.
● Work with CTIRU ‘the police assessed list of unlawful terrorist content, produced on behalf of the Home Office’	🟩	Securly integrates and block unlawful terrorist content using the list provided by the UK Home Office and Met Police CTIRU (Counter-Terrorism Internet Referral Unit).
● Confirm that monitoring for illegal content cannot be disabled by the school	🟩	All illegal content categories are locked at a system level. Schools cannot disable these filters.

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Illegal	content that is illegal, for example child abuse images and unlawful terrorist content	🟩	Illegal content such as CTIRU list of terrorist content and IWF list of child abuse content are both built into Securly Filter for blocking and monitoring.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others	🟩	Securly Aware's 'Think Twice' cyberbullying prevention widget promotes responsibility and digital citizenship. Think Twice prompts students to reconsider before they send hurtful messages by automatically detecting bullying in typed text and presenting the student with a message immediately. Securly uses AI-powered heuristic tools to provide built-in sentiment analysis which detects bullying content, emails, web searches and social media posts. Securly will flag bullying activity in real-time to enable intervention.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet	🟩	Securly is an IWF member and fully CIPA compliant. Access to known child abuse and exploitation sites is prevented.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity	🟩	Securly provides a "Hate" category which allows administrators to block access and alert on websites and content which promote hatred and discrimination across race, religion, age, or sex.

Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	Securly provides a “Drugs” category which allows administrators to block access and alert on websites and content which include details of manufacture, sale, and distribution.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	Securly includes the CTIRU illegal terrorist content blocklist and provides a “Hate” category. This allows administrators to block access and alert on websites and content which includes promote terrorist organisations and actions, violence and intolerance.
Gambling	Enables gambling	🟩	Securly provides a “Gambling” category which allows administrators to block access and alert on websites and content that promotes betting or risky actions for a reward.
Pornography	displays sexual acts or explicit images	🟩	Securly provides a “Pornography” category which allows administrators to block access and alert on websites that contain pornographic or explicit images and media.
Self Harm	promotes or displays deliberate self harm	🟩	Securly Aware uses AI sentiment analysis to detect self-harm content, emails, web searches and social media posts. Alerts are categorised under the terms ‘Self-harm’ and ‘Grief’ Securly will flag activity from vulnerable students in real-time to enable emergency intervention.

Suicide	Suggest the user is considering suicide	🟩	Securly uses AI sentiment analysis which detects content that suggests suicidal ideation in emails, web searches, online docs, and social media posts. Alerts are categorised under the terms ‘Self-harm’ and ‘Grief’ Securly will flag activity from vulnerable students in real-time to enable emergency intervention.
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	Securly uses AI sentiment analysis which detects violent language towards others in emails, web searches, online docs, and social media posts. Alerts are categorised under the terms ‘Violence’ Securly will flag activity from vulnerable students in real-time to enable emergency intervention.

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

Securly Filter categories include keywords/phrases, URLs and domains of over the top one million websites.

- Securly PageScan provides automated categorisation of previously unknown websites by scanning the page content and images.
- Selective HTTPS man-in-the-middle decryption to provide real-time, URL filtering, keyword filtering and sentiment analysis.
- Our customers can provide their own block and allow lists in policies and can submit any websites for inclusion in our categories.

Unlike traditional on-premise filtering solutions Securly will selectively intercept to block and filter content. This prevents over blocking or problems with safe content and education services online.

Previously unknown or uncategorised websites will be analysed by Securly Pagescan to accurately determine their content and determine if they need to be filtered.

Administrators also have ability to manage their own safe sites and override Securly categorised websites.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
● Age appropriate – includes the ability to implement variable monitoring appropriate to age and vulnerability. This will in turn define which alerts are prioritised and responded to. Further situations may warrant additional capability, for examples boarding schools or community based access	🟩	Securly can be configured to use GSuite OUs or Azure/EntraID Groups to define separate filtering policies appropriate to different ages or roles. (E.g. Staff, Primary Students, Senior Students).
● Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided	🟩	Alerts can be configured at a global level, as well as on a per-policy level. Staff groups can be configured to receive instant alerts about specific groups of students. Administrators can configure scheduled reports to selected users.

● Audit – Any changes to the monitoring system are logged enabling an audit trail that ensures transparency and that individuals are not able to make unilateral changes.	🟩	Securly administrators can permit or deny by using their own domain names and keywords globally or per policy. Any changes to the system are logged in an audit trail. Reports that are exported from the system are logged separately within the system.
● BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supported and how data is managed. Does it monitor beyond the school hours and location	🟩	BYOD devices on school premises can be monitored using Guest Network policies. BYOD are sometimes enrolled in management systems and could have filtering applied to them whilst off-site although this is not typical.
● Data retention –what data is stored, where is it (physically– ie cloud/school infrastructure) stored and for how long. This should also include any data backup provision	🟩	All log data is stored securely within Securly's cloud infrastructure. Measures are taken to ensure compliance with local laws and regulations such as GDPR and DPA. EU customer data resides solely within the EU. Data retention is not currently limited but can be removed at a customer's request.
● Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers	🟩	Securly is network based solution and no client-side software is required. Securly is device and operating system agnostic.
● Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy	🟩	Administrators can edit policies to include their own custom keywords to allow, block or alert on.

● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	As a cloud-based service, the Securly Safety Console is available anywhere with Internet access. Delegated control can be provided to additional administrators or Safeguarding teams. Multiple sites and take-home policies can all be managed from the same central dashboard. For large school trusts or partners managing filtering for multiple schools, Securly’s Multi-School Dashboard provides a dropdown that lets the admin switch across different schools without having to log in separately each time.
● Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?	🟩	We recommend schools allow for monitoring within their own Acceptable Usage Policy and IT policies so all users are aware. Securly can assist by providing templates and training webinars on what should be included.
● Multiple language support – the ability for the system to manage relevant languages?	🟩	Securly implements multiple language support for both filtering and management interface in English, French, and Spanish. Language support is being continually developed and additional languages will be added as available.
● Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?	🟩	Securly flag high priority issues in their “flagged” reporting section and alerts are triggered immediately. Additionally, the Securly On-call team can provide additional human review of alerts around the clock and notify emergency contacts or authorities in highest risk cases.

● Remote monitoring – with many children and staff working remotely, the ability, extent and management for the monitoring of devices (school and/or personal). Included here is the hours of operation together with the explicit awareness of users.	🟩	Securly Filter can be applied to school owned devices regardless of how they access the internet or whether they are within the school network. Securly Filter can also be applied to BYOD schemes, and Guest networks ensuring all devices using the school broadband connection are appropriately filtered.
● Reporting – how alerts are recorded within the system?	🟩	As well as email all alert events are also recorded to the web dashboard reports or flagged activity section.
● Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)	🟩	Securly Aware automatically recall emails containing violence, bullying, or nudity and quarantine images for review by a designated safeguarding lead.

Pro Active Monitoring - how any pro-active monitoring support is provided including if any automation is utilised and the safeguarding capability of the organisation's teams.

Securly offers institutions a range of preventative tools to support student safeguarding and wellness.

Securly Aware creates a Student Wellness Level for ever user. SLT or DSLs can quickly identify the students who are trending negatively, drill down into individual student's wellness levels and gain insight into contributing online activities (with Filter). Proactively investigate students who are trending negatively, and provide preventative support and intervention before they become extreme risks

Securly Aware's 'Think Twice' cyberbullying prevention widget promotes responsibility digital citizenship. Think Twice, prompts students to reconsider before they send hurtful messages.

Wellness Widget Intervention. When a student's Wellness Level drops, the Wellness Pathways widget will automatically present helpful resources to them on their screen.

Recall emails and quarantine images. Securly Aware automatically recall emails containing violence, bullying, or nudity.

Securly are a Student Safety company and are concerned with wellbeing of students beyond web filtering;

- Securly Aware - Student safety and wellness solution that provides unprecedented visibility into your students' mental health and wellness. Google Drive files, One Drive files, emails, social media, and web searches are scanned to identify indications of suicide, depression, violence, bullying, and nudity.
- On-call - Enlist a team of expert analysts to manage your school's Aware alerts and notify you if a student needs help now
- Securly Home - Parent app, a free feature included with your school's Filter purchase, giving parents control over their child's school device when it goes home, including web filtering, site restrictions, and monitored screen time.
- Classroom - Classroom management tool that works seamlessly across Chrome, Windows, and Mac.

Please note below opportunities or enhancements to support schools (and other settings) with their obligations around Keeping Children Safe in Education?

Securly is a student safety company and provides services beyond web filtering and student wellness monitoring.

- On-Call - Enlist a team of expert analysts to manage your school's Aware alerts and notify you if a student needs help now

- Training sessions and material provided to Schools to help follow best practice and integrate Securly technology into their safeguarding procedures.

Securly Filtering and Monitoring Annual Review

- Strategic reviews of filtering and monitoring policies
- Review of adequate filtering and monitoring procedures
- Data assessment and insights: activity, alerts and safeguarding trends

Securly implements multiple language support for both filtering and management interface in English, French, and Spanish.

Securly administrators can permit or deny by using their own domain names and keywords globally or per policy.

Staff members assigned to Faculty Groups can now edit policies that affect OUs or Security Groups assigned to them. This feature can be enabled and disabled at an admin level.

Any changes to the system are logged in an audit trail.

Securly's filtering policies are customisable and policy changes can be applied to specific user groups by the administrator, so that overlocking doesn't occur for certain student groups if they are researching legitimate areas to do with sexual health for due to the requirements of the RHSE and PSHE curriculum.

Monitoring 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	Jarrett Volzer
Position	VP of Product
Date	03/08/2023
Signature	Jarrett Volzer