# Appropriate Monitoring for Schools

## Monitoring Provider Checklist Reponses

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. 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."

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 Inc |
|---|---|
| Address | 111 N. Market Street, 4th floor, Suite 400<br>San Jose, California 95113<br>United States |
| Contact details | https://www.securly.com/contact-us |
| Monitoring System | Securly Filter |
| Date of assessment | 19/10/2018 |

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 are a member of the Internet Watch Foundation since 2016. |
| ● Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' | | Securly work closely with Met Police CTIRU and Home Office and integrate the police assessed list of unlawful terrorist content in Securly filter. |

## 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 uses AI and machine learning 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 provide 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 provide a "Drugs" category which allows administrators to block access and alert on websites and content which include details of manufacture, sale, distribution, |

| | | | and recreational use of illegal substances. |
|---|---|---|---|
| Extremism | promotes terrorism and terrorist ideologies, violence or intolerance | | Securly include the CTIRU illegal terrorist content blocklist and provide a "Hate" category. This allows administrators to block access and alert on websites and content which include promote terrorist organisations and actions, violence and intolerance. |
| Pornography | displays sexual acts or explicit images | | Securly provide a "Pornography" category which allow 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 uses AI and machine learning to provide built-in sentiment analysis which detects self-harm content, emails, web searches and social media posts.<br><br>Securly will flag vulnerable persons activity in real-time to enable intervention. |
| Suicide | Suggest the user is considering suicide | | Securly uses AI and machine learning to provide built-in sentiment analysis which detects content, emails, web searches and social media posts that suggest a person is considering suicide.<br><br>Securly will flag vulnerable persons activity in real-time to enable intervention. |
| Violence | Displays or promotes the use of physical force intended to hurt or kill | | Securly's AI sentiment analysis will detect and flag violent content. Flagging violent activity as high priority to registered Safeguarding contacts. |

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.

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

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. 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 Google or Microsoft Active Directory organisational units (OUs) 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 | | Email alerts are configurable can be delegated to other staff members such as Safeguarding team.<br><br>Delegated user can also access a portal to run reports and further investigate incidents.<br><br>Securly's 24 Team provide around the clock monitoring of high priority alerts. |

| | | |
|---|---|---|
| 🎬 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.<br><br>SecurlyHome can also extend monitoring outside of School hours and premises, including parental involvement in Safeguarding their children. |
| 🎬 Data retention –what data is stored, where is it (physically) stored and for how long | | All log data is stored securely within Securly's cloud infrastructure.<br><br>Measures are taken to ensure compliance with local laws and regulations such as GDPR and DPA. EU customer data resides solely within the EU.<br><br>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 solutions and no client-side software is required. Securly is device and operating system agnostic. |
| 🎬 Flexibility – schools ability to amend (add or remove) keywords easily | | 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, Securly's management interface is available anywhere with Internet access.<br><br>Delegated control can be provided to additional administrators or Safeguarding personnel.<br><br>Multiple sites and take-home policies can all be managed from the same central dashboard. |

| | | |
|---|---|---|
| 🎬 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 AUP and IT policies so all users are aware.<br><br>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 currently supports English language. Support for additional languages is due early 2019. |
| 🎬 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.<br><br>Additionally, Securly24 team can provide additional human review of alerts around the clock and notify emergency contacts or authorities in highest risk cases. |
| 🎬 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. |

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

Securly are a Student Safety company and provide services beyond email and web filtering.
- Securly24: A dedicated team of trained student safety coordinators provide 24/7 monitoring of alerts and support to schools own safeguarding team.
- Training sessions and material provided to Schools to help follow best practice and integrate Securly technology into their safeguarding procedures.

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 selfcertification 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 | Chris Humby |
|------|-------------|
| Position | Securly UK Consultant |
| Date | 19/10/2018 |
| Signature | _CHumby_ |