Appropriate Monitoring for Schools

UK Safer Internet Centre
www.saferinternet.org.uk
brought to you by SWGfL Childnet IWF

June 2018

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	eSafe Global Limited
Address	New Court, Regents Place, Manchester
Contact details	Email: hello@esafeglobal.com Tel: 08443 443 001 Website: www.esafeglobal.com
Monitoring System	eSafe Service
Date of assessment	September 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	🟩	eSafe is a member of the IWF
● Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	eSafe collaborates with the Home Office and directly with regional Police Prevent teams to identify markers of localised risk. These are incorporated into the dynamic eSafe Threat Libraries to provide visibility of terrorist related risk at a granular, local level. See eSafe Service summary section below

Inappropriate Online Content

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

Content	Explanatory notes –	Rating	Explanation
Illegal	content that is illegal, for example child abuse images and unlawful terrorist content	🟩	eSafe employs sophisticated pure image and keyword detection technology together with our constantly updated Threat Library to capture evidence of a wide range of illegal behaviour, in school and beyond, irrespective of the application or language in use. Child abuse and paedophile activity is often detected from webcam analysis, sometimes on encrypted applications, and illegal static imagery which is not supported by text. In excess of 95% of all child abuse imagery associated with successful prosecutions in the UK has no text associated with it, therefore moving and static image analysis, agnostic of the application, is critical. Unlike alternative monitoring solutions, eSafe's pure image detection engine intelligently reads an image to determine its content. eSafe's unparalleled ability to monitor in any language, including any script, ensures that unlawful written content is detected, irrespective of whether it is viewed to screen, entered via the keyboard, accessed or downloaded from a USB or mobile device. The review of all incidents detected by the specialist behaviour monitoring at eSafe ensures that evidence of actual illegal content or behaviour is escalated by phone call, in real-time, to a nominated contact.

Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others	🟩	The detection, review and escalation of all safeguarding risk comprises the 3 TripleLock components mentioned above and outlined in the Summary section below. In respect of bullying behaviour, eSafe's Threat Libraries contain thousands of dynamically maintained bullying related words, contextual phrases, euphemisms and slang, in multiple languages, reflecting culturally specific terms that would be meaningless in English, in addition to localised markers specific to an individual school or region. eSafe engages with organisations who are specialist practitioners in a particular field of behaviour. This enables eSafe to source new markers of threats, and create additional markers internally - based on evidence of current trends. In this way the eSafe Service provides an unmatched detection capability across a wide range of safeguarding risk – see Summary section below.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet	🟩	See responses to the behaviours above and the summary section below. Child Sexual Exploitation is generally evidenced by imagery, chat, social media and webcam activity, often on encrypted applications such as Skype. The early warning markers of such behaviour are often very subtle and require an expert eye to detect. The multi-lingual team of behaviour specialists at eSafe provide both the essential expert review and the immediate escalation of genuine risk, 24 x7, 365 days per year.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity	🟩	See responses to the behaviours above and the Summary section below. Also note that the multi-lingual monitoring can be critical in identifying discrimination and that genuine risk is often masked by large volumes of false positives. The specialist review of all incidents, in all languages ensures that genuine discrimination, even with cultural bias, is identified
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	See responses to the behaviours above and the Summary section below. Also note that substance abuse is a behaviour typically associated with a vast number of constantly changing euphemisms and terms, as users attempt to disguise their activity. A newly identified term is added to the eSafe Threat Library to ensure that all eSafe school and college customers throughout the UK (and internationally) benefit from that marker on the same day. In this way as a term grows in popularity, the eSafe detection algorithms are dynamically updated to ensure the behaviour marker is visible at an eSafe school or college.

Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	See responses to the behaviours above and the Summary section below. Also note the critical importance of multi-language monitoring and regularly updated Threat Libraries to ensure effective detection of all aspects of extremist risk. In addition, extremism and the grooming of individuals by extremists is often associated with very subtle, and seemingly benign behaviour, occurring over an extended period of time. The specialist monitoring resources employed at eSafe have both the subject matter expertise and the time to review incidents in context and cross reference with historic activity involving the same user. In this way, genuine risk can be identified from a series of low level, seemingly benign incidents that may otherwise go unnoticed. It is also eSafe's experience that serious extremist risk is more likely revealed by offline activity and use of devices away from school or college. Material is typically passed via USB to read offline and the activity is conducted away from the school or college premises.
Pornography	displays sexual acts or explicit images	🟩	See responses to Illegal and Child Sexploitation above and the Summary section below. eSafe's sophisticated image detection capability will identify moving, static and webcam pornographic material, online or offline, irrespective of the application used. Our experience and evidence of monitoring 1,000,000+ students and staff in the UK shows that pornographic images and videos are frequently downloaded to school and college devices from pen drives and mobile phones. Sexual acts are performed on webcam and encrypted applications such as Skype. Pornographic material is stored by users on school and college hard drives and central storage areas, hidden in innocent folders. Even if an image is not opened for viewing by the user, eSafe scans local and central drives to identify stored pornography ensuring that a school or college can be confident such material is always visible and the appropriate intervention made.

Self Harm	promotes or displays deliberate self harm	🟩	See responses to the behaviours above and the Summary section below. Mental health related issues such as anxiety, depression, self-harm and suicide risk represents the single largest category of incidents detected by eSafe across students and staff - at all levels of education in the UK. This is a behaviour which can include image-based evidence but certainly is typified in its early stages by subtle markers which require expert interpretation and assessment. eSafe prides itself on the early warning of self-harm risk which is a direct result of: • the time and effort the team places on ensuring that our Threat Library markers are extensive and current; • the continuous engagement with specialist organisations in the field of mental health. eSafe is a member of the Association of Child and Adolescent Mental Health (ACAMH); • the subject matter expertise across our highly trained eSafe monitoring team • the multi-lingual incident review by eSafe monitoring staff 24 x 7, 365 days per year; • the breadth and quality of our detection capability in identifying offline and offsite behaviour conducted in any language.
Suicide	Suggest the user is considering	🟩	See the response to Self-Harm above and the Summary section below.
Violence	Displays or promotes the use of physical force	🟩	See the responses above and the Summary section below.

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

eSafe Monitoring Service Summary

eSafe recognises the increasing responsibility that school and college leaders have for safeguarding children and young people in their care. especially with the latest guidance from the Department for Education (Sept 2018) stipulating that schools and colleges should do all that they reasonably can to limit children's exposure to the risks while putting in place early intervention strategies to help to stop safeguarding risks escalating.

In this context, **eSafe takes the strain of detecting safeguarding risks** with a unique Monitoring Service built around a TripleLock approach that provides highly effective behaviour identification, not just during term time and school or college hours, but 24 hours a day, 365 days a year**.**

The eSafe service comprises a unique TripleLock approach:

1. **Advanced detection software** - with the capability to monitor both words and phrases, as well as images that are moving *and* static.
    - Safeguarding risk may be wholly or partly written in a foreign language script, a foreign language written using an English keyboard (Romanised), include slang or text-speak variants, or reflect a cultural meaning which doesn't translate to English. eSafe has a unique ability to detect risks in any language, in any text.
    - The markers of many serious threats are often imagery based, typically moving imagery, on webcam, chat roulette and encrypted applications like Skype. In fact, 95% of imagery associated with child abuse and paedophile activity has no text associated with it at all. With sophisticated image detection technology, eSafe ensures that static, video and webcam activity - which is not accompanied by text or meta data - is visible too.

2. **Expert interpretation & assessment** - Effective incident review demands time to examine monitoring output and specialist knowledge to interpret the signs. A dedicated team of behavioural experts work diligently to identify the early warning indicators of inappropriate and harmful behaviour. Importantly, the team is multi-lingual with a rich knowledge of different cultures - vital skills for interpreting and assessing the true meaning of words, phrases, slang and text speak in different languages.

    With *eSafe* all incidents detected are reviewed by the *eSafe* team, categorised into various levels of seriousness and escalated through to the school by phone and encrypted email to a pre-agreed protocol. Depending upon the nature of the incident or issue, the escalation may go to a single individual (e.g. illegal image to safeguarding lead or a Head teacher only) or to a combination/group of contacts (e.g. accessing porn in Year 9 to Year leader & safeguarding lead).

3. **Dynamic Threat Libraries - updated continuously by the eSafe InsightLab to maintain detection accuracy** - working in collaboration with external partners and schools, our experts update and refine threat libraries on a daily basis to detect emerging behavioural trends at an international, national and local level.
    - The eSafe Threat Libraries comprise tens of thousands of markers across multiple languages
    - Words and phrases are monitored against a series of Libraries covering threats of illegal and inappropriate behaviours, *such as grooming, paedophile activity, child abuse and sexualisation, bullying and harassment, possible self- harm/suicide, HBT, FGM, racism, radicalisation, threats of violence, terrorist activity, trafficking and gang culture.*
    - The Libraries are updated daily to maintain detection accuracy and reflect changes in behaviour trends. New markers are sourced from continuous research by our monitoring experts as well as through close collaboration with external specialist agencies and schools. For example, the intelligence gathered from our sex offender monitoring work on behalf of UK Police Forces is used to ensure the grooming and paedophile threat library is always up to date.
    - Schools also benefit from eSafe's global and national library footprint e.g. an issue emerging a day ahead in Australia is added to the relevant Threat Library before the next

UK academic day; a marker related to trafficking risk identified in a local region of the UK is added to the Threat Library to aid detection across all schools in that area. This level of responsiveness ensures that schools benefit quickly from monitoring of current and very diverse indicators of safeguarding risk.

- In addition, eSafe maintains and administers bespoke Threat Libraries for individual schools to cope with issues such as gang culture, local slang and requirements for specialist behavioural detection.

Monitoring 24/7, 365 days a year

To effectively fulfil statutory safeguarding duties, school leaders have to maintain visibility of ICT use whenever and wherever it is deployed. School devices are regularly taken off site by students and staff for use at home during evenings, weekends and holidays. In fact, our evidence shows that 1/3 of incidents happen offline – often in the evenings, weekends and holidays

Most traditional monitoring software solutions, and all filtering solutions that offer a degree of keyword detection, are often focused on online activity, usually on site. This means that the significant volume of incidents that happen offline - in the evenings, weekends and holidays - are invisible to the safeguarding team.

With eSafe, incidents that happen out of hours are reviewed 24/7, 365 days a year - and those requiring immediate intervention are escalated in real-time to ensure effective intervention, protection and support for the individual, and minimal reputation risk for the school.

Focused on finding the early markers of harmful and inappropriate behaviours, however subtle

The DfE states that you must have early visibility of markers of harmful and inappropriate behaviours, so that intervention strategies can be put in place to stop the risk from escalating.

The problem is, the markers associated with the range of safeguarding risks can often be incredibly subtle. The content is likely to be very benign: the obvious markers of risk will be absent and the safeguarding threat easily overlooked.

Self-administered solutions place an increasing burden on a school's resources if the required level of safeguarding is to be attained. Even with highly accurate detection technology, high volumes of false positives are produced and every incident must be checked - in context with historic activity. Applying weighting to terms or relying on machine intelligence to identify issues affecting welfare and wellbeing in such a dynamically changing environment as human behaviour, can easily lead to vast volumes of false positive incidents, and actual evidence of risk being completely overlooked.

The specialist team at eSafe has the time and necessary skill to assess the severity of incidents and - importantly - to distinguish between the genuine issues (requiring intervention) and the false positives. This not only removes the burden other systems place on non-specialists, it ensures the very serious incidents are not lost under a blanket of false positive and less serious data.
The high volume of false-positives associated with traditional software monitoring solutions often forces schools to adopt a 'top10' approach, focusing on incidents by volume. In an attempt to manage the volume of activity that comes through, markers can be removed. It is vital that experienced and trained specialists make these decisions based on a robust volume of evidence.

At eSafe we recognise that the ICT environment is a rich source of behaviour markers and believe, therefore, it is important that all incidents are reviewed. Typically, the more serious behaviours do not occur in volume and a ‘top 10’ approach or the removal of a marker can easily result in the complete loss of visibility of a serious safeguarding risk. Large volumes of benign incidents easily mask the single subtle marker of life threatening behaviour, or illegal activity, and at eSafe all incidents are reviewed by experts skilled in behaviour monitoring.

Each team member at eSafe shares a passion for safeguarding and:

- *Holds a degree in at least one of the following areas: Child Psychology, Criminology, Forensic Science and Computing Forensics.*
- *Has experience of working with and supporting young people and adults in a variety of behaviour related situations e.g. bullying and harassment, grooming, child abuse, mental health, offender management.*
- *Has on-going training across the range of inappropriate or harmful behaviours.*
- *Is DBS checked and security vetted to NPPV (Non Police Personnel Vetting) 3 as a minimum, but with many holding Security Clearance (SC), Counter Terrorism Clearance (CTC) and Developed Vetting (DV) status*

eSafe provides accurate baseline measurement that makes the assessment of intervention strategies straight forward

The DfE (and Inspectorate) requires that when intervention plans are put in place, the effectiveness is measured and used to refine future intervention strategy.

eSafe provides analysis of actual and genuine behaviour to illustrate the effectiveness of interventions as the baseline changes over time.

The trouble with the reports typically provided by traditional software-based monitoring solutions is the significant volume of false positives that are included in the data, as they cloud the genuine underlying incident baseline.

The monthly, termly and annual reports and analysis provided by eSafe only reflect incidents that have been reviewed by our specialist team and require intervention. Meaning the baseline of behaviour and safeguarding risk is accurate, enabling the leadership team to correctly assess the effectiveness of their interventions and plan future intervention strategies accordingly.

How does it work?

The eSafe application is securely installed on the school computer device(s), in the cloud (e.g. Google Chrome), or on servers controlling such as thin client and virtual desktop environments (VDI) - to monitor a user’s online (Internet) and offline activity, both in school and away from the school network. Each computer device can be uniquely identified in its environment, and the user is allocated to a specific group to aid granular monitoring and reporting e.g. staff, student, year group, vulnerable or site specific.

When potentially inappropriate behaviour is flagged to the team at eSafe via the application, this is what happens:

- The incident is captured as a screen shot

- A screen shot is uploaded to an eSafe server along with the user id, machine name, time and date stamp.
- The incident is reviewed by the specialist behavbiour team at *eSafe*, located in physically secure, Police approved, ISO27001 accredited monitoring laboratory facility in Manchester.
    - Incidents requiring intervention are identified and escalated to nominated contacts using the pre-agreed escalation/reporting protocol.
    - Serious incidents (e.g. child abuse imagery, grooming, life threatening behaviour) are reported by telephone, directly to the specified safeguarding contact(s) in real-time.
- An encrypted report is produced, including supporting material where appropriate, and sent by email - stating the user id, machine id, time/date of the incident captured and a narrative of the incident.
- If the school or college uses CPOMS, the incident report can be automatically delivered into the school CPOMS application

The data captured by eSafe in the course of monitoring users is protected during transmission and at rest:

- All data transmitted between a school/college device & the eSafe server is encrypted (256 AES)
- The eSafe servers are located behind a secure firewall at a UK based ISO27001 accredited data centre
- Access to the servers is password controlled
- Access to the eSafe application on the servers is password controlled
- Data is validated upon receipt to prevents code insertion attacks.
- Database access is password protected and the data 'at rest' in the database is encrypted to provide another level of database obfuscation

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

The eSafe monitoring service is geared to ensure that the ‘blocking’ of content is appropriate and does not restrict legitimate activity. Blocking can be applied to:

- Content e.g. an image blocked but not written content
- Document, file or URL blocked entirely based on pre-defined criteria e.g. it is on a published banned list, known to be unlawful, contains inappropriate material such as pornography or radical comment etc,
- Applications e.g. Chatroulette, Social Media Gaming, Tor browser
- Device e.g. attempts to access an inappropriate file/content held on a pen drive

Blocking can be applied at school, user group, device group, user and device level as the school or college requires.

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	🟩	Monitoring can be configured to individual user and user group level to reflect variable monitoring of applications, websites, and behaviour, appropriate to age. In addition, monitoring settings can be applied to a specific device or groups of devices, and the settings governed by a time-based schedule if necessary. In this way, eSafe delivers variable monitoring to suit specific requirements at user, group or site level based on age, time of day (e.g. senior boarders can access PEGI 12 rated games but only outside normal school hours) All incidents are reviewed by eSafe behaviour analysts and prioritisation of incident escalation will be dependent upon the escalation and reporting protocol agreed with the specific school.

• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided	🟩	See Monitoring Service Summary above
• 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	🟩	eSafe offers a variety of approaches to monitor BYOD. Whether the BYOD is monitored beyond school hours and location is dependent on the requirements agreed with the device owner. If a parent only wants their child's device to be monitored during school hours or when in school, monitoring settings will be applied accordingly. BYOD monitoring can be achieved by: (i) Deployment of the eSafe client software to the personal device with the permission of the device owner (ii) Connection of the BYOD to the school network via Thin Client (Terminal Services or VDI) (iii) Connection of the BYOD to the school G-Suite environment All incident data is managed as set out in the eSafe Monitoring Service summary above in accordance with legislative requirements.

• Data retention –what data is stored, where is it (physically) stored and for how long	🟩	When an incident occurs, the data captured by eSafe comprises a screen shot, user login id, device id, time and date stamp, behaviour reviewer narrative, and various device component identifications. The data is encrypted on the device and transmitted to the eSafe server located at a ISO 271001 accredited, UK Police approved, data centre in the UK. The data is validated to prevent code insertion attacks and further encrypted at rest in the server database to provide another level of obfuscation. Data access is restricted to authorised eSafe employees. Data retention periods are determined by the customer, or in the instance of an illegal incident, the Police.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers	🟩	Software does not need to be installed on the device as eSafe can also monitor in the Cloud (e.g. G-Suite) or via Thin Client channels (e.g. Terminal Server TS or Virtual Desktop VDI). However, on average 30% of all markers of safeguarding risk occur offline, therefore to ensure visibility, a device capable of operating offline should be installed with the eSafe monitoring client. Supported operating systems include: • Windows • MACOS • Chrome • Android
• Flexibility – schools ability to amend (add or remove) keywords easily	🟩	See Monitoring Service Summary above. The eSafe InSight Lab administers the keyword Threat Library and new terms can added within minutes of identification. The eSafe Client Services team works proactively with schools and colleges to identify localised terms and phrases relevant to individual sites. The eSafe InSight Lab also controls the removal of terms. Schools using self-administered monitoring solutions often remove terms to limit false positives without appreciating the significance of the marker in identifying low volume, serious safeguarding risk. eSafe is monitoring approximately 1m pupils and staff across the UK (Aug 2018) and we have unparalleled visibility of the relevance of terms. In this way only truly redundant terms are removed.

• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	eSafe is a multi-site managed Service. We centrally monitor over 1m users across approximately 2000 schools and colleges. Multi-campus colleges, Academy Trusts and Local Authority deployments are common, with eSafe delivering monitoring and reporting to specific to individual group/multi-site requirements.
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?	🟩	It is the responsibility of a school to make users aware that their use of the schools' digital environment is being monitored. eSafe can force user policy acceptance at login to aid schools reminding users. The eSafe Client Services team supports schools and colleges in communicating monitoring policy and the transition to the eSafe Service with guidance and collateral.
• Multiple language support – the ability for the system to manage relevant languages?	🟩	See responses above and eSafe Monitoring Service summary. eSafe is able to technically able to recognise any language script; the eSafe Threat Libraries are maintained to reflect culturally specific markers; and eSafe employs behaviour analysts with language skills to correctly assess and interpret foreign language incidents in context.

• 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?	🟩	See eSafe Monitoring Service summary above. Analysis of each incident is performed by the eSafe Behaviour Analyst and its severity assessed. Escalation of issues is via real-time phone call to nominated school contacts, and daily and weekly encrypted reports The escalation of safeguarding risk is determined by the reporting and escalation protocol agreed with each customer school, MAT/Group or Local Authority. Within each school/college the protocol is flexible to allow the escalation of specific categories of risk and the monitoring of individuals, to be tailored. One school may require bullying to be reported by phone escalation to the headteacher for the current term, whereas the next school may want bullying escalated as a standard daily report. Similarly, all incidents, regardless of severity, involving a vulnerable pupil may need to be escalated to a specific nominated contact at the school.
• Reporting – how alerts are recorded within the system?	🟩	In addition to the incident data captured by eSafe – see Data Retention above, the incident report generated for the school or college is archived on the server. Each incident is assigned a category flag to reflect the behaviour identified, which feeds graphical and tabular incident analysis for the school or college, illustrating trends over time and the impact of intervention..

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

The range of safeguarding risks that children and young people in education may potentially face is broad, with mental health issues being particularly prevalent, but incidents are rising across all categories. The latest KCSiE guidance reinforces the need for early help across all areas of safeguarding risk but emphasises peer on peer abuse, sexual violence and harassment in particular.

As such, accurate detection and assessment of harmful, inappropriate or illegal behaviours to ensure fast, early intervention and support, is vital.

However, risk markers can often be incredibly subtle. They tend to form an overall pattern of seemingly isolated incidents over time - and the identification of a pattern or single incident that does require intervention needs dedicated time as well as specialist knowledge and understanding.

Often more serious safeguarding risks, such as grooming, abuse and radicalisation, are evident on webcam and encrypted applications like Skype, and are increasingly detected through image monitoring alone. eSafe's unique Pure Image Detection Technology monitors static imagery, video, streaming and webcam activity.

Detection software must be continuously refreshed. After all, risks can only be detected when the terminology (markers) associated with the behaviours is actually known and can be employed by the software detection algorithms. Think about how quickly the language we use develops and how trends come and go: the pace of change means we're adopting more words, phrases, abbreviations and slang terms faster than ever before and, because of social media, these are moving around the world within days and weeks. That's why eSafe's Insightlab team works tirelessly to keep our Threat Libraries up to date, adding new terms and phrases every day and removing those that become redundant. Our own extensive research, and collaboration with our clients and specialist agencies, ensures that we can identify the local, national and international behaviour trends and all the associated markers to enable us to do this.

For over 1m children and young people in education in the UK, English is a second language. And the markers of safeguarding risks will often be unique to a specific culture and ethnic community.
Our combination of intelligent detection software, expert human behaviour analysis and dynamic threat libraries (which include behaviour markers across multiple languages), means eSafe is unique in being able to detect risks in any language and script. Importantly, our multi-lingual monitoring team have a rich knowledge of different cultures, enabling them to interpret and assess the true meaning of words, phrases, slang and text speak in different languages.

Effective safeguarding requires continuous measurement of the outcomes of interventions.
The reporting element of eSafe has an important role in providing a baseline of behaviours for this measurement, helping to illustrate the effectiveness of interventions as the baseline changes over time. Importantly, the eSafe analysis only reflect incidents that have been certified as genuine by our specialist Behaviour Analysts. This means the baseline of behaviour and safeguarding risk is accurate; enabling you to correctly assess the effectiveness of interventions and plan future strategies accordingly.

The most forward-thinking schools and colleges take a holistic view on safeguarding strategy; one which encompasses everything from spotting and acting on early risk signs to proactively promoting good emotional health and wellbeing for all. By choosing eSafe, educational leaders can use the data gathered to focus their efforts where they are most needed; shaping the pastoral agenda to suit their own particular challenges around culture and attitudes.

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	Mark Donkersley
Position	Managing Director
Date	3rd September 2018
Signature	Mark Donkersley