Appropriate Monitoring for Schools

June 2017

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	IT Solutions 4 all Ltd.
Address	4 Cheviot Drive, Shepshed, Leics, LE12 9ED
Contact details	Chris Smith
Filtering System	Monitoring using Future Digital Software
Date of assessment	13/09/17

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		Yes, Future Digital is a member of IWF
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Yes, Future Digital has integrated the Police assessed list.

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		The software works by monitoring for, recording and alerting of predefined words and phrases that are categorised against a theme and level of potential risk.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		Same as above – directly relates to pre-defined word and phrase themes – *Racism & Violence* and *Acronyms*.
Child Sexual Exploitation	: Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Same as above – directly relates to pre-defined word and phrase themes – *Pornography*, *Predators* & *Strangers* and *Acronyms*
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Same as above – directly relates to pre-defined word and phrase themes – *Racism & Violence* and *Acronyms*.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Same as above – directly relates to pre-defined word and phrase theme – D*rugs and Addiction*
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Same as above – directly relates to pre-defined word and phrase theme – *Prevent*
Pornography	displays sexual acts or explicit images		Same as above – directly relates to pre-defined word and phrase theme - *Pornography*, *Predators* & *Strangers* and *Acronyms*
Self Harm	promotes or displays deliberate self harm		Same as above – directly relates to pre-defined word and phrase theme – *Self Harm and Suicide*
Suicide	Suggest the user is considering suicide		Same as above – directly relates to pre-defined word and phrase theme – *Self Harm and Suicide*
Violence	Displays or promotes the use of physical force intended to hurt or		Same as above – directly relates to pre-defined word and phrase

	kill		theme - *Racism & Violence*

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

ITS4all allows for peace of mind by offering a highly effective Active Monitoring Service for Future Digital's products which takes place daily over 24 hours whether the device is in or out of school, throughout the whole year. The service was designed by the ITS4all Managing Director in 2007 and over the years has developed to meet the demands of schools and Government Strategies whilst safeguarding a school's digital activity.

ITS4all use Future Digital's products which are designed to monitor for-predefined word and phrases based on themes. Themes have been developed with multi-agency support so that instances of risk can be identified. Future Digital's software features an auto pre-grading facility whereby each word is categorised with a level of risk from 1-5. 1 is the lowest level of risk and often refers to a false/positive capture while 5 is the highest level. Captures are initially categorised in this way in order to ensure that the highest risk captures are identified instantaneously and thus ensure targeted action by the ITS4all Data Monitors. The words and phrases that are monitored can be typed or viewed and come from any application on the device, not just online from the internet.

Each incident triggered by the software is captured as a screen shot which is time and date stamped, identifies the device and identifies the logged on user.

ITS4all data monitoring experts all have experience of working at a senior level in schools and Local authorities, hold a qualification in computer forensics and are CEOP ambassadors and enhanced DBS cleared. The Data Monitors categorise and grade incidents and escalate causes of concern to Head Teachers or safeguarding personnel identified by the educational establishment.

ITS4all also provides bi-monthly eSafety Reports for each establishment as well as a bi-monthly technical report for IT Technicians. We also offer continued initial technical support and training for the software.

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

The system has the capability to block words and websites dependent on school specific requirements however, its primary purpose is to monitor for activity and behaviour related to risk and not to limit children and young people's activity in the e-learning environment.

ITS4all manage the system on behalf of schools and their own particular requirements.

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		The system is entirely customisable and can be set to respond to different groups dependent on criteria such as age.
• 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		Future Digital's software can be utilised for iPad by using our safe browser, Futures Browser. This would need to be installed on a student's device by the school and activity monitored through the Future Digital console. Please note to use this solution all other browsers such as Safari, Chrome, Firefox would need to be disabled. The installed client will continue to monitor beyond school hours and location.
• Data retention –what data is stored, where and for how long		Futures Cloud uses Microsoft Azure to provide its cloud technology. Data is stored in Data Centres within Northern Europe. Data is retained for 365 days.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		Full monitoring is provided on any device running Windows or Mac.
• Flexibility – schools ability to amend (add or remove) keywords easily		As data controllers, schools have full control over keywords contained within Future Digital's themes. The only exception to this is the Prevent (developed in relation to the *Prevent* Duty) which is hard coded in to the software and therefore
• Monitoring Policy – How are all users made		Future Digital's advises

aware that their online access is being monitored? Is any advice or guidance provided to support schools?		schools to ensure that students are made aware of the presence of monitoring software as part of the school's Acceptable Use Policy at computer login.
• Multiple language support – the ability for the system to manage relevant languages?		The custom libraries allow for the addition of words and phrases using English keyboard characters, in alternative languages. In addition the support of alternative scripts is planned with Arabic support due in 2017.
• 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?		Futures Cloud prioritises information based on a scoring algorithm. The result of this is that potential higher risk information can be delivered proactively to data monitors by an alerting system, proactive reports or via a customisable real time dashboard. ITS4all data monitors review all captures and grade accordingly. Incidents requiring intervention are reported immediately to the designated contact.
• Reporting – how alerts are recorded within the system?		Future Digital's reporting can be customised to send scheduled reports at regular intervals to designated members of staff. In addition user interfaces within the Future Digital console are designed to visually highlight instances of risk at a glance. ITS4all produce bi-monthly reports for all schools with complete information and comprehensive details on how to interpret the information correctly.

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

- ITS4all's fully active monitoring service is fully scalable meaning that no matter how large or small your establishment we can provide you with the most cost-effective solution ensuring that the cost is directly proportionate with potential risk at your particular school.

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	Chris Smith
Position	Managing Director
Date	13/09/17
Signature