

# E-Safety Policy

---

## Sponsorship & Review

### 1 Sponsor

Assistant Vice Principal for Safeguarding

### 2 Reviewed

August 2023

### 3 Revised

September 2023

## Social Media Policy

Charlton School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online. E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility. Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our behaviour policy.

### 1. Roles and responsibility

The School e-Safety Coordinator is Assistant Vice Principal for Safeguarding, Angela Bithell

The designated member of the governing body responsible for e-safety is Ricki Thiara

### 2. Communicating school policy

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PSHEE lessons where personal safety, responsibility, and/or development are being discussed.

### 3. Making use of ICT and the internet in school

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life,

education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school. Some of the benefits of using ICT and the internet in schools are:

#### **For students:**

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

#### **For staff:**

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking

## **4. Learning to evaluate internet content**

With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiarism very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the school e-safety coordinator. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively. (Appendix 1)

## 5. Managing information systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the IT technicians and network manager and virus protection software will be updated regularly.

Some safeguards that the school takes to secure our computer systems are:

- ensuring that all personal data sent over the internet or taken off site is encrypted
- making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- files held on the school network will be regularly checked for viruses
- the use of user logins and passwords to access the school network will be enforced
- portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

For more information on data protection in school please refer to our data protection policy. More information on protecting personal data can be found in section 11 of this policy.

## 6. Emails

The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication. It is also used to enhance the curriculum by:

- initiating contact and projects with other schools nationally and internationally
- providing immediate feedback on work, and requests for support where it is needed. Staff and pupils should be aware that school email accounts should only be used for school-related matters, ie for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

### 6.2 School email accounts and appropriate use

Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school. Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:
  - in school, pupils should only use school-approved email accounts
  - excessive social emailing will be restricted
  - pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
  - pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge. Pupils will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

## 7. Published content and the school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects. The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only. For information on the school policy on children's photographs on the school website please refer to section 7.2 of this policy.

### 7.2 Policy and guidance of safe use of children's photographs and work

Colour photographs and pupils work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school's policy on the use of photographs of children, including:

- how and when the photographs will be used
- how long parents are consenting the use of the images for
- school policy on the storage and deletion of photographs.

Parents will be contacted annually for consent.

Using photographs of individual children The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place. It is important that published images do not identify students or put them at risk of being identified. The school is careful to ensure that images published on the school website cannot be reused or manipulated through watermarking and browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

Parental consent must be obtained.

Consent will cover the use of images in:

- all school publications or on the school website
  - in newspapers as allowed by the school
  - in videos made by the school or in class for school projects.
- 
- Electronic and paper images will be stored securely.
  - Names of stored photographic files will not identify the child.
  - Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (ie a student in a swimming pool, rather than standing by the side in a swimsuit).
  - For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
  - Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
  - Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
  - Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and

will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our school child protection and safeguarding policy.

### 6.3 Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our complaints policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools child protection and safeguarding policy and behaviour policy.

### 6.4 Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school/There are various restrictions on the use of these sites in school that apply to both students and staff. Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHEE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

## 8. Mobile phones and personal device

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make pupils and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined in our mobile devices policy.

## 9. Cyberbullying

Cyberbullying, as with any other form of peer on peer abuse, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the behaviour policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. If an allegation of bullying does come up, the school will:

- take it seriously
- act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- record and report the incident
- provide support and reassurance to the victim
- make it clear to the 'bully' that this behaviour will not be tolerated.

If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions. If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school. Repeated bullying may result in a fixed-term exclusion.

## 10. Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.



## 11. Protecting personal data

Charlton School believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision. We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect. For more information on the school's safeguards relating to data protection read the school's data protection policy.

### [Appendices](#)

# Appropriate Filtering for Education settings



June 2021

## Filtering Provider Checklist Responses

Schools 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, 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 they “should be doing all that they reasonably can to limit children’s exposure to the above 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.”

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to “have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content.”

By completing all fields and returning to UK Safer Internet Centre ([enquiries@saferinternet.org.uk](mailto:enquiries@saferinternet.org.uk)), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined ‘appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Renato Software Ltd.
Address	11 High Street, Ruddington, Nottingham, NG11 6DT
Contact details	0115 857 3776 Sales@renatosoftware.com
Filtering System	Senso® Filter Cloud
Date of assessment	09/06/2021

## 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.	

## Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
<ul style="list-style-type: none"><li>• Are IWF members</li></ul>		Senso® is a member of the IWF and actively communicate with them.
<ul style="list-style-type: none"><li>• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)</li></ul>		IWF Lists are provided updated within Senso via an API
<ul style="list-style-type: none"><li>• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'</li></ul>		CTIRU URL Lists are provided and updated in real time within Senso via an API

## Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		Discrimination Category is one of 500 + unique content categories, and includes daily and real-time updates, as well as ActiveWeb traffic from over 600+ million end users globally with 99% ActiveWeb Coverage and Accuracy
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Several categories combine to cover Drugs & Substance Abuse Categories as above
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Extremism category as above plus Daily updates of the CTIRU URL lists
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Yes – covered within Malicious Internet Activity Category
Pornography	displays sexual acts or explicit images		Adult Content Category included as above
Piracy and copyright theft	includes illegal provision of copyrighted material		Covered within Criminal Activity / Piracy Category

Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Self Harm Category included as above
Violence	Displays or promotes the use of physical force intended to hurt or kill		Weapons / Violence category included as above

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

More than 99% active web coverage and accuracy  
Web traffic from 600+ million end users globally  
Over 200 languages supported  
Daily and real-time updates  
Senso's filter cloud not only benefits from extensive category-based libraries to block inappropriate websites, but also uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained.

We have a basic filter package which doesn't include logging of internet history, and a premium package including logging of internet history. The latter retains logs currently from the date of installation for the length of a customers active subscription.

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

Senso as a provider work closely with partners and customers to ensure the filter is appropriately blocking harmful and inappropriate content without over blocking. Customers have the option to both schedule and turn off completely specific categories such as social media and gaming, based on age or role within the school, to allow for a flexible and strategic approach to internet use. Senso also provides the ability to whitelist any websites which are blocked by Senso Filter Cloud on the fly, as required by the individual customer.

## Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> <li>Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role</li> </ul>		Ability to : Schedule All / some categories Group web filtered users by criteria such as staff / year group with options

		to allow certain categories at certain times and have different strengths of filter.
<ul style="list-style-type: none"> <li>• Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.</li> </ul>		Senso will block access to torrent repositories, proxy anonymisers, peer to peer file sharing sites to support protection against circumvention.
<ul style="list-style-type: none"> <li>• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content</li> </ul>		Ability to add wild card words or URL's to Senso Filter as required. Turn on and off filter categories. Whitelist URL's.
<ul style="list-style-type: none"> <li>• Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked. For example, being able to contextually analyse text on a page and dynamically filter</li> </ul>		Senso's filter cloud not only benefits from extensive category-based libraries to block inappropriate websites, but also uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries
<ul style="list-style-type: none"> <li>• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking</li> </ul>		Yes.
<ul style="list-style-type: none"> <li>• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard</li> </ul>		Scalable and flexible to support multi-site right down to individual user unique filtering policy.
<ul style="list-style-type: none"> <li>• Identification - the filtering system should have the ability to identify users</li> </ul>		Users are identified upon log on to the device.
<ul style="list-style-type: none"> <li>• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)</li> </ul>		Senso Filter Cloud is available on iOS devices and soon to be android. This will work in a similar way from a flexibility perspective.
<ul style="list-style-type: none"> <li>• Multiple language support – the ability for the system to manage relevant languages</li> </ul>		Over 200 languages supported

<ul style="list-style-type: none"> <li>Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)</li> </ul>		<p>Senso has moved to the hybrid classroom and typical on premise network filtering no longer provides the flexible approach to onsite and remote learning required by UK education. Filter Cloud is cloud and client based filtering, designed to support devices which may move on and off the school network.</p>
<ul style="list-style-type: none"> <li>Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school</li> </ul>		<p>As above, with the option to schedule the Senso Filter Cloud to turn on once a device leaves the network or at specific times.</p>
<ul style="list-style-type: none"> <li>Reporting mechanism – the ability to report inappropriate content for access or blocking</li> </ul>		<p>If a user accesses an inappropriate site, the customer can instantly add this to their block list via Key Word Libraries.</p>
<ul style="list-style-type: none"> <li>Reports – the system offers clear historical information on the websites visited by your users</li> </ul>		<p>Yes in the premium Filter Cloud Package, all websites visited by users are logged within Senso.</p>

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to *“consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum”*.<sup>1</sup>

Please note below opportunities to support schools (and other settings) in this regard

#### Senso Safeguard Cloud :

Cloud based, real time monitoring of activity on school owned devices, designed to highlight to school staff users who may be vulnerable or at risk to themselves, at risk to others or behaving inappropriately. Senso indicates a potential concern by raising a “violation” when a keyword, acronym or phrase typed, matches against those found within our libraries. The violation information including a screenshot can then be viewed in the dashboard by the relevant Senso Safeguarding Portal User. The screenshot will also be analysed by our AI driven image analysis to indicate whether a student is potentially viewing harmful or inappropriate content alongside the keyword typed. This helps with prioritisation of Senso violations.

Integrates with CPOMS & Myconcern

<sup>1</sup> <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

Live Dashboard to support proactive and strategic online safeguarding

Senso Concern Reports (included with Senso Safeguard Cloud) :

The ability for users to anonymously report a concern about themselves or someone else and include a screen capture if required.

Senso Safeguarding for Microsoft Teams App:

Monitors all Microsoft Teams Chat regardless of device or location a user is logged on. Will also analyse images alongside the chats to identify users who may be vulnerable or at risk to themselves, at risk to others or behaving inappropriately. Senso indicates a potential concern by raising a “violation” when a keyword, acronym or phrase typed, matches against those found within our libraries. The violation information including chat transcript can then be viewed in the dashboard by the relevant Senso Safeguarding Portal User. All images sent within Microsoft Teams chat will also be analysed by our AI driven image analysis to indicate whether a student is potentially sending harmful or inappropriate images.

Senso Assisted Monitoring Service:

A fully managed service with human screening/moderation/assessment including external escalation, real-time evaluation of events by safeguarding experts with effective and expert triage, with phone calls for most serious cases for instant attention.


Senso Class Cloud

Tools and monitoring for teachers to ensure focused and engaging lessons, whether they or a student are logged in at school or remotely.

## 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	Michael Payne
Position	Directors of Operations
Date	26-Aug-2021
Signature	



# Appropriate Filtering for Education settings



June 2021

## Filtering Provider Checklist Responses

Schools 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, 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 they “should be doing all that they reasonably can to limit children’s exposure to the above 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.”

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to “have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content.”

By completing all fields and returning to UK Safer Internet Centre ([enquiries@saferinternet.org.uk](mailto:enquiries@saferinternet.org.uk)), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined ‘appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Smoothwall
Address	Avalon, 1 Savannah Way, Leeds Valley Park, Leeds, LS10 1AB, UK
Contact details	<a href="https://www.smoothwall.com/education/contact-us/">https://www.smoothwall.com/education/contact-us/</a>
Filtering System	Smoothwall Filter
Date of assessment	8 <sup>th</sup> July 2021

## 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.	

## Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
<ul style="list-style-type: none"><li>• Are IWF members</li></ul>		Yes, Smoothwall are a member of the Internet Watch Foundation and implement the IWF CAIC list.
<ul style="list-style-type: none"><li>• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)</li></ul>		Smoothwall implement the IWF CAIC list of domains and URLs. Smoothwall Filter also uses a number of search terms and phrases provided by IWF and their members. We perform self-certification tests daily to ensure that IWF content is always blocked through a Smoothwall Filter.
<ul style="list-style-type: none"><li>• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'</li></ul>		Smoothwall Filter implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.

## Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		The 'Intolerance' category covers any sites which promote racial hatred, homophobia or persecution of minorities. Sites which advocate violence against these groups are also covered by the Violence category.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		The Drugs category covers the sale, manufacture, promotion or use of recreational drugs as well as abuse of prescription drugs. Sites which provide resources which aim to help those suffering from substance abuse are covered by the 'Medical Information' category. Sites which discuss Alcohol or Tobacco are covered by the 'Alcohol and Tobacco' category.

Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		The 'Terrorism' category contains the 'police assessed list of unlawful terrorist content'. Smoothwall also provides both a 'Violence' category which covers violence against both animals or people; An 'Intolerance' category (covered further above) and a 'Gore' category which covers any sites which describe or display gory images and video.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		As well as providing a level of protection against externally created malware, Smoothwall Filter provides a Hacking category which includes sites such as "how to" on hacking, and sites encouraging malicious computer use. Filter bypass tools are covered separately in a comprehensive "web proxies" category, which uses a combination of domain lists and dynamic content analysis.
Pornography	displays sexual acts or explicit images		The 'Pornography' category contains sites containing pornographic images, videos and text. Sites which contain mild nudity for purposes other than sexual arousal are covered by the 'Non-Pornographic Nudity' category. The 'Pornography' category uses both a list of domains/URLs as well as dynamic content rules which ensure new, previously unseen sites can be identified on the fly.
Piracy and copyright theft	includes illegal provision of copyrighted material		The 'Piracy and Copyright Infringement' category contains sites which illegally provide copyright material or provide peer-to-peer software.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		The 'Self Harm' category contains sites relating to self-harm, suicide and eating disorders. The category excludes sites which aim to provide medical or charitable assistance which are categorised as 'Medical Information' or 'Charity and Non-Profit' respectively.

Violence	Displays or promotes the use of physical force intended to hurt or kill		The 'Violence' category contains sites which advocate violence against people and animals. We also provide a 'Gore' category which contains images and video of gory content.
----------	---	--	---

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

As well as the categories listed above, Smoothwall Filter provides filtering and reporting for over 100 other categories ranging from 'Sexuality Sites' and 'Non-Pornographic Nudity' through to 'News', 'Sport' and 'Online Games'.

Smoothwall Filter uses a wide variety of techniques in order to identify and categorise content. All categories use a list of both URLs and domains, with the majority of categories also using search terms, content-based rulesets, and regular expressions to identify content on the fly.

Smoothwall have an in-house Digital Safety Team which are responsible for maintaining and updating the site categorisation rules which are released to customers on at least a daily basis; ensuring that schools are always protected from the latest threats.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained .

Retention policies when using on-premise reporting are set by customer preference (and limited by size of disk). Smoothwall will assist customers in specifying the correct hardware for their desired retention. Customers are encouraged to discuss with Smoothwall their retention requirements when using Cloud Reporting, for which the standard retention is 3 months.

All loglines are identified by the users directory username unless an on-premise device is not configured with authentication.

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

What is and is not blocked depends primarily on the policies specified by the customer. However, the underlying categorisation is highly granular, and assesses the content of pages. This uses an intelligent rules-based mechanism rather than automatically categorising a site as "pornography" for only one mention of "porn" on a page. This intelligence allows sites to be more accurately classified and filtered upon, without unduly restricting access.

Furthermore, while these same underlying categories are also used for identifying sites for the purpose of Smoothwall's Safeguarding suite of tools, a site may be allowed according to the filtering policy, but still be flagged as a potential issue in Safeguarding reports. This means a school can provide access to a large proportion of the internet, while also keeping an eye on content accessed by pupils. With this degree of visibility and awareness, pupils can be educated rather than merely ring-fenced.

## Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> <li>Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role</li> </ul>		Smoothwall Filter integrates with a wide variety of directories (e.g. Microsoft AD, Azure AD, Google Directory) allowing filtering to be set appropriately at group and user level.
<ul style="list-style-type: none"> <li>Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.</li> </ul>		Smoothwall maintains an extensive rules database for detecting circumvention activity. VPNs must also be blocked by a firewall – Smoothwall's optional Firewall uses Layer 7 analysis to identify non-web VPN traffic.
<ul style="list-style-type: none"> <li>Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content</li> </ul>		Smoothwall Filter has a full range of policy tools available, allowing School users to easily make policy changes, test a site against current policy or simply quickly allow or block a site.
<ul style="list-style-type: none"> <li>Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked. For example, being able to contextually analyse text on a page and dynamically filter</li> </ul>		All downloaded content (http and https) is analysed in real-time and dynamically categorised by the Smoothwall filter. Private content, such as banking sites, may be excluded from this dynamic filter.
<ul style="list-style-type: none"> <li>Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking</li> </ul>		Smoothwall maintains a “blocklist policy document” which includes clear criteria on what should and should not be in each category. This is available on request.
<ul style="list-style-type: none"> <li>Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard</li> </ul>		Smoothwall products allow for multi-tenant deployments, where a central unit controls policy and reporting. Delegated access is available. Smoothwall can work in a cluster as well as a standalone unit.

<ul style="list-style-type: none"> <li>• Identification - the filtering system should have the ability to identify users</li> </ul>		Smoothwall Filter offers a wide range of techniques for identifying users – including negotiate authentication, login pages and RADIUS compatibility, as well as a number of custom options.
<ul style="list-style-type: none"> <li>• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)</li> </ul>		Any app content delivered via HTTPS (not necessarily through a web browser) can be blocked and inspected by Smoothwall, assuming the app permits this. In addition, Smoothwall's optional firewall module can identify and block many other types of app.
<ul style="list-style-type: none"> <li>• Multiple language support – the ability for the system to manage relevant languages</li> </ul>		Smoothwall's combined blocklist include words in a wide variety of languages, focussed on those spoken in UK and US schools. This includes Polish and Spanish as well as "non latin" such as Urdu and Russian.
<ul style="list-style-type: none"> <li>• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)</li> </ul>		Smoothwall Filter offers both network level filtering, and device based filtering, for use as appropriate.
<ul style="list-style-type: none"> <li>• Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school</li> </ul>		Smoothwall's Cloud Filter provides identical filtering capabilities to the on-premise system including dynamic, contextual content filtering.
<ul style="list-style-type: none"> <li>• Reporting mechanism – the ability to report inappropriate content for access or blocking</li> </ul>		Smoothwall provides the ability to report overblocked content to the administrator. Uncategorized content (which is possibly "underblocked") is automatically fed back to Smoothwall and will subsequently be appropriately categorized.
<ul style="list-style-type: none"> <li>• Reports – the system offers clear historical information on the websites visited by your users</li> </ul>		Smoothwall Filter offers a comprehensive suite of reports and logs, with a complete URL-by-URL record

		of all web activities including timestamp, username and source device. Logs are retained to customer preference.
--	--	--

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to *“consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum”*.<sup>1</sup>


Please note below opportunities to support schools (and other settings) in this regard

Smoothwall partners with National Online Safety to provide education materials for young people around online safety. Customers should speak to their Customer Success manager if they would like to find out more information.

#### 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	Tom Newton
Position	Head of Product
Date	8 <sup>th</sup> July 2021
Signature	

<sup>1</sup> <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

# Telford & Wrekin IDT Managed Services



## Keeping Children Safe in Education Filtering and Monitoring

### Telford and Wrekin IDT Services Response October 2022



Services  
for schools



[www.twccommercial.co.uk](http://www.twccommercial.co.uk)  
[servicesforschools@telford.gov.uk](mailto:servicesforschools@telford.gov.uk)  
01952 380522

Contact us to discuss your requirements



# Filtering and Monitoring

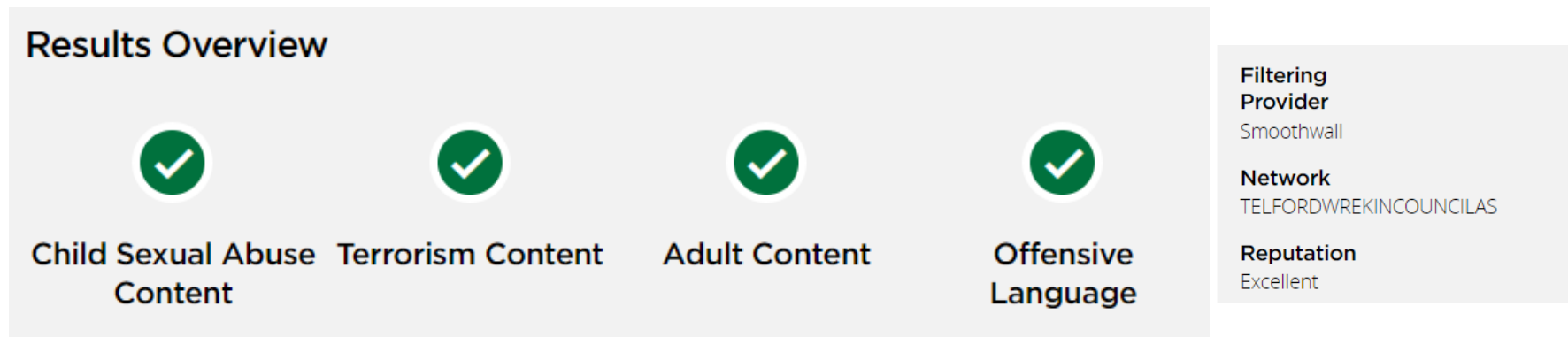
- Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system.
- As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness

# How do IDT meet this requirement?

- Internet Filtering Provision: Smoothwall



- This blocks access to any of the material listed below
- Using the DfE recommended testing site by SWGfL here are the results:-



# How do IDT meet this requirement?

## Child Sexual Abuse Content



**Blocked**

### Description

Tests whether you are blocking websites on the IWF Child Abuse Content URL list.

### Results & Recommendations

It appears that your filtering solution includes the IWF URL Filter list, blocking access to Child Sexual Abuse content online

## Terrorism Content



**Blocked**

### Description

Tests whether you are blocking websites on the Counter-Terrorism Internet Referral Unit list (CTIRU).

### Results & Recommendations

It appears that your filtering solution includes the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online

## Adult Content



**Blocked**

### Description

Test whether your Internet filter blocks access to pornography websites

### Results & Recommendations

It appears that your filtering solution includes blocking for online pornography

## Offensive Language



**Blocked**

### Description




Accesses a page containing offensive language to test if your filtering software blocks it

### Results & Recommendations

It appears that your filtering solution includes blocking for offensive language





# UK Safer Internet Checklist

## Illegal Online Content

Aspect	Rating	Explanation
Are IWF members		Yes, Smoothwall is a member of the Internet Watch Foundation and implements the IWF CAIC list
and block access to illegal Child Abuse Images(by actively implementing the IWF URL list)		Smoothwall implements the IWF CAIC list of domains and URLs. Smoothwall Filter also uses a number of search terms and phrases provided by IWF and their members. We perform self certification tests daily to ensure that IWF content is always blocked through a Smoothwall Filter
Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Smoothwall Filter implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office






# UK Safer Internet Checklist

## Inappropriate Online Content

Aspect	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		The 'Intolerance' category covers any sites which promote racial hatred, homophobia or persecution of minorities. Sites which advocate violence against these groups are also covered by the Violence category.
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances		The Drugs category covers the sale, manufacture, promotion or use of recreational drugs as well as abuse of prescription drugs. Sites which provide resources which aim to help those suffering from substance abuse are covered by the 'Medical Information' category. Sites which discuss Alcohol or Tobacco are covered by the 'Alcohol and Tobacco' category.
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance		The 'Terrorism' category contains the 'police assessed list of unlawful terrorist content'. Smoothwall also provides both a 'Violence' category which covers violence against both animals or people; An 'Intolerance' category (covered further above) and a 'Gore' category which covers any sites which describe or display gory images and video.
Malware / Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		As well as providing a level of protection against externally created malware, Smoothwall Filter provides a Hacking category which includes sites such as "how to" on hacking, and sites encouraging malicious computer use. Filter bypass tools are covered separately in a comprehensive "web proxies" category, which uses a combination of domain lists and dynamic content analysis.

# UK Safer Internet Checklist

## Inappropriate Online Content

Aspect	Explanatory notes – Content that:	Rating	Explanation
Piracy and copyright theft	Includes illegal provision of copyrighted material		The 'Piracy and Copyright Infringement' category contains sites which illegally provide copyright material or provide peer-to-peer software.
Self Harm	Promotes or displays deliberate self harm (including suicide and eating disorders)		The 'Self Harm' category contains sites relating to self-harm, suicide and eating disorders. The category excludes sites which aim to provide medical or charitable assistance which are categorised as 'Medical Information' or 'Charity and Non-Profit' respectively
Violence	Displays or promotes the use of physical force intended to hurt or kill		The 'Violence' category contains sites which advocate violence against people and animals. We also provide a 'Gore' category which contains images and video of gory content
Pornography	Display ssexual acts or explicit images		The 'Pornography' category contains sites containing pornographic images, videos and text. Sites which contain mild nudity for purposes other than sexual arousal are covered by the 'Non-Pornographic Nudity' category. The 'Pornography' category uses both a list of domains/URLs as well as dynamic content rules which ensure new, previously unseen sites can be identified on the fly.
Multiple language support – the ability for the system to manage relevant languages			Smoothwall's combined blocklist include words in a wide variety of languages, focussed on those spoken in UK and US schools. This includes Polish and Spanish as well as "non latin" such as Urdu and Russian.

# How to IDT meet this requirement?




- Classroom Monitoring Provision: Senso



- More than 99% active web coverage and accuracy  
Web traffic from 600+ million end users globally. Over 200 languages supported Daily and real-time updates. Senso's filter cloud not only benefits from extensive category-based libraries to block inappropriate websites, but also uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries

# UK Safer Internet Checklist









## Illegal Online Content

Aspect	Rating	Explanation
Are IWF members		Senso® is a member of the IWF and actively communicate with them.
and block access to illegal Child Abuse Images(by actively implementing the IWF URL list)		IWF Lists are provided updated within Senso via an API
Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		CTIRU URL Lists are provided and updated in real time within Senso via an API



# UK Safer Internet Checklist

## Inappropriate Online Content

Aspect	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		Discrimination Category is one of 500 + unique content categories, and includes daily and real-time updates, as well as ActiveWeb traffic from over 600+ million end users globally with 99% ActiveWeb Coverage and Accuracy
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances		Several categories combine to cover Drugs & Substance Abuse Categories as above
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance		Extremism category as above plus Daily updates of the CTIRU URL lists
Malware / Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Yes – covered within Malicious Internet Activity Category
Pornography	Display ssexual acts or explicit images		Adult Content Category included as above
Piracy and copyright theft	Includes illegal provision of copyrighted material		Covered within Criminal Activity / Piracy Category
Self Harm	Promotes or displays deliberate self harm (including suicide and eating disorders)		Self Harm Category included as above
Violence	Displays or promotes the use of physical force intended to hurt or kill		Weapons / Violence category included as above

# How to IDT meet this requirement?

- Senso Safeguard Cloud :
- Cloud based, real time monitoring of activity on school owned devices, designed to highlight to school staff users who may be vulnerable or at risk to themselves, at risk to others or behaving inappropriately. Senso indicates a potential concern by raising a “violation” when a keyword, acronym or phrase typed, matches against those found within our libraries.
- The violation information including a screenshot can then be viewed in the dashboard by the relevant Senso Safeguarding Portal User. The screenshot will also be analysed by our AI driven image analysis to indicate whether a student is potentially viewing harmful or inappropriate content alongside the keyword typed. This helps with prioritisation of Senso violations.
- Integrates with CPOMS & Myconcern - If your school would like this integration please log a call on the IDT portal or speak to your IDT Gold Technician.



The banner features a collage of four small photographs on the left showing students in a classroom setting. To the right of these photos is a large orange rectangle containing the text 'Services for schools' in white. Further right, there is a black rectangle containing contact information in white text.

Services  
for schools

[www.twccommercial.co.uk](http://www.twccommercial.co.uk)  
[servicesforschools@telford.gov.uk](mailto:servicesforschools@telford.gov.uk)  
01952 380522

Contact us to discuss your requirements