



# Online safety and Cybersecurity Policy

Last updated:	Oct 2023
Approved by Governors:	13.12.23
Review cycle:	Annual
Review date:	12.12.24

## 1. Introduction

Effective online safety and security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. This policy aims to respond to this requirement and is informed by the Department for Education (DfE) guidance, Keeping Children Safe in Education, and the Digital and Technology Standards and therefore applicable for schools and colleges in England. This Online Safety Policy is based on guidance from SWGFL and The Key for School Leaders and has been developed with senior leaders in school, including the DSL, and with the support of teachers, LSAs and technical staff. The policy is ultimately reviewed and approved by Governors.

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools to pupils and staff, including staff understanding of the expectations and responsibilities in relation to filtering and monitoring
- A school's responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners
- Acceptable internet use and particularly preventing and tackling bullying and cyber-bullying <https://www.gov.uk/government/publications/searching-screening-and-confiscation>

It also refers to the DfE's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

## 3. Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of High Ash to safeguard members of our school community online in accordance with statutory guidance and best practice. It applies to all members of the school community (including staff, pupils, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school.

Our approach to online safety is based on addressing the following categories of risk as defined in Keeping Children Safe in Education 2003.

1. **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
2. **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
3. **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
4. **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels
- is published on the school website.

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place.

## **4. Responsibilities**

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

### **4.1 The governing board**

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The governing board will:

- make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- ensure children are taught how to keep themselves and others safe, including keeping safe online and that where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness.
- review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards.
- Receive (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

## **4.2 The Headteacher**

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

## **4.3 Designated Safety Lead (DSL)**

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the Cybersecurity and online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

## **4.4 Online Safety Lead**

The Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
  - content

- contact
- conduct
- commerce

#### 4.5 Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme e.g. [ProjectEVOLVE](#) .

This will be provided through:

- PHSE and SRE programmes
- a mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#).

#### 4.6 Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Cybersecurity and Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement
- they immediately report any suspected misuse or problem to the OSL and DSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Cybersecurity and Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, such as Chrome books etc., in lessons and other school activities and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

#### 4.7 IT Provider/Technical Support

It is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Cybersecurity and Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Cybersecurity and Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority
- there is clear, safe, and managed control of user access to networks and devices

- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies.

#### 4.8 Pupils

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

#### 4.9 Parents and carers

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Cybersecurity and Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)

#### 4.10 Visitors and members of the community

Visitors (including contractors, agency workers and volunteers) and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

## 5. Acceptable use of the internet in school

### 5.1 Acceptable use

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

The school will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where

appropriate. The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

The Cybersecurity and Online Safety Policy and acceptable use agreements define acceptable/unacceptable use at school. The acceptable use agreements will be communicated/re-enforced through:

- pupil diary
- staff induction and handbook
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website

### Acceptable use

Consideration should be given for the following activities when undertaken for non-educational purposes:	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	X				X			
Online shopping/commerce			X	X	X			
File sharing		X			X			
Social media			X	X	X			
Messaging/chat			X	X			X	
Entertainment streaming e.g. Netflix, Disney+			X	X	X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok			X	X			X	
Mobile phones may be brought to school		X			X			
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school		X			X			
Taking photos on mobile phones/cameras			X	X			X	
Use of other personal devices, e.g. tablets, gaming devices			X	X	X			
Use of personal e-mail in school, or on school network/wi-fi			X	X	X			
Use of school e-mail for personal e-mails			X	X	X			

## Unacceptable use

<p>Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:</p>	<p><b>Any illegal activity for example:</b></p> <ul style="list-style-type: none"> <li>• Child sexual abuse imagery*</li> <li>• Child sexual abuse/exploitation/grooming</li> <li>• Terrorism</li> <li>• Encouraging or assisting suicide</li> <li>• Offences relating to sexual images i.e., revenge and extreme pornography</li> <li>• Incitement to and threats of violence</li> <li>• Hate crime</li> <li>• Public order offences - harassment and stalking</li> <li>• Drug-related offences</li> <li>• Weapons / firearms offences</li> <li>• Fraud and financial crime including money laundering</li> </ul>
<p>Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)</p>	<ul style="list-style-type: none"> <li>• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)</li> <li>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> <li>• Creating or propagating computer viruses or other harmful files</li> <li>• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)</li> <li>• Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>• Using penetration testing equipment (without relevant permission)</li> </ul>
<p>Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:</p>	<ul style="list-style-type: none"> <li>• Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)</li> <li>• Promotion of any kind of discrimination</li> <li>• Using school systems to run a private business</li> <li>• Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school</li> <li>• Infringing copyright</li> <li>• Unfair usage (downloading/uploading large files that hinders others in their use of the internet)</li> <li>• Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute</li> </ul>

When using communication technologies, the school considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community

- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff.*

## **5.2 Cyber-bullying**

### ***Definition***

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### ***Preventing and addressing cyber-bullying***

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

## **5.3 Reporting and responding**

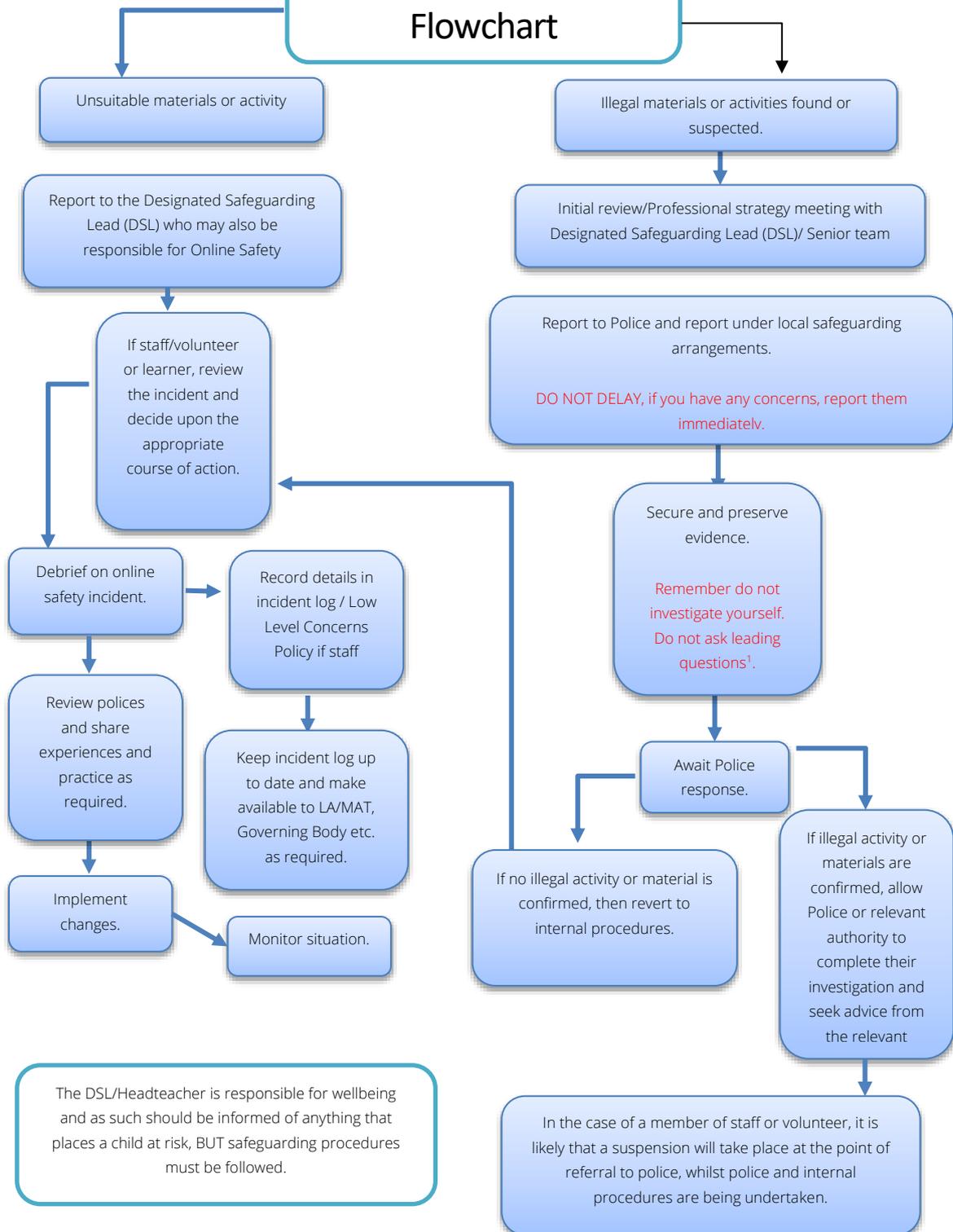
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents.
- reports will be dealt with as soon as is practically possible once they are received.
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and trained to deal with online safety risks.

- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm ([see flowchart and user actions chart in the appendix](#)), the incident must be escalated through the agreed school safeguarding procedures, this may include:
  - Non-consensual images
  - Self-generated images
  - Terrorism/extremism
  - Hate crime/ Abuse
  - Fraud and extortion
  - Harassment/stalking
  - Child Sexual Abuse Material (CSAM)
  - Child Sexual Exploitation Grooming
  - Extreme Pornography
  - Sale of illegal materials/substances
  - Cyber or hacking offences under the Computer Misuse Act
  - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- where there is no suspected illegal activity, devices may be checked by at least two members of senior staff/governor

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

# Online Safety Incident Flowchart



The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

#### 5.4 School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows

#### Responding to Learner Actions

Incidents	Refer to class teacher	Refer to Headteacher	Refer to Police/Social Work/Local authority	Inform parents/carers	Remove device/network/internet access	Further warning/sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in <a href="#">earlier section on User Actions</a> on unsuitable /inappropriate activities).		X	X			
Corrupting or destroying the data of other users.	X	X		X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X			X		
Using proxy sites or other means to subvert the school's filtering system.	X	X				
Accidentally accessing offensive or pornographic material and failing to report the incident.	X			X		
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X	X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X		X		
Unauthorised use of digital devices (including taking images)	X	X		X		
Unauthorised use of online services	X	X		X		
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X		X		
Continued infringements of the above, following previous warnings or sanctions.						X

## Responding to Staff Actions

Incidents	Refer to line manager / Headteacher	Refer to local authority HR	Refer to Police	Refer to technical Support Staff for action re filtering, etc.	Issue a warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	X	X	X	X		
Deliberate actions to breach data protection or network security rules.	X	X		X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X		X		
Using proxy sites or other means to subvert the school's filtering system.	X	X		X		
Unauthorised downloading or uploading of files or file sharing	X			X		
Breaching copyright or licensing regulations.	X			X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X	X		X	X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X		X	X	X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X			X	X	
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X			X	X	
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X			X		
Actions which could compromise the staff member's professional standing	X			X	X	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X		X	X	X
Failing to report incidents whether caused by deliberate or accidental actions	X			X		
Continued infringements of the above, following previous warnings or sanctions.		X		X	X	X

## 6 Online Safety Education

### 6.1 Pupils

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected World Framework by UKCIS/DCMS and the SWGfL, JIGSAW and regularly taught in a variety of contexts.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- Incorporates/makes use of relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#)
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people.

## **6.2 Staff Training**

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations

## **6.3 Governors**

A higher level of training will be made available to (at least) the Cybersecurity and Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.
- Governors should take part in online safety training/awareness sessions, with particular importance for those who are involved in technology/online safety/health and safety/safeguarding.

## **6.4 Families**

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- the children – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
- Concerns or queries about this policy can be raised with any member of staff or the headteacher.

## 7. Technical security

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The management of technical security is the responsibility of Governors and Senior Leaders, supported in this by the Designated Safeguarding Lead, Online Safety Lead and IT Service Provider. The school's procedures should ensure:

- users can only access data to which they have right of access
- access to personal data is securely controlled in line with the school's personal data policy
- system logs are maintained and reviewed to monitor user activity
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems, including filtering and monitoring provision

### 7.1 Implementation

The school is responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements as set out by the Department for Education in relation to
  - Broadband provision
  - Wireless network
  - Cabling
  - Filtering and monitoring
  - Cloud storage
  - Servers and storage

<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges>

- cyber security is included in the school risk register.
- there will be regular reviews and audits of the safety and security of school technical systems.
- servers, wireless systems, and cabling must be securely located and physical access restricted.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- appropriate security measures (including updates) are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems.
- the school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff
- all users will have clearly defined access rights to school technical systems and accounts are deleted when the user leaves.

- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security (*see password section below*)
- The IT Service Provider, in partnership with Governors/SLT/DSL, regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement. The school is currently using Smoothwall for filtering and monitoring
- an appropriate system is in place for pupils and class teachers to report any actual/potential technical incident to the SLT/DSL/Online Safety Lead (OSL)
- The Online Safety Lead is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations and that the latest software updates (patches) are applied.
- personal data should be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- supply teachers users are provided with appropriate access to school systems based on an identified risk profile.

## **7.2 Password Security**

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform)..

- The password policy and procedures reflect NCSC and DfE advice/guidance.
- Security measures are in place to reduce brute-force attacks and common passwords are blocked.
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- For younger children and those with special educational needs, learner usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- Learners are encouraged to set passwords with an increasing level of complexity. Passwords using 3 three random words and with a length of over 12 characters are considered good practice.
- Users will be required to change their password if it is compromised
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

## 8. Filtering and Monitoring

The DfE outlines that schools should have filtering system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content and a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged. Roles and responsibilities for the management of filtering and monitoring systems should be defined and allocated and the provision is reviewed at least annually and checked regularly.

### 8.1 Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. Where available, schools should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies and provide training and awareness raising to help users understand the process that is available to them.

The school's filtering system should be operational, up to date and applied to all:

- users, including guest accounts.
- school owned devices
- devices using the school broadband connection.

The school's filtering system should:

- filter all internet feeds, including any backup connections.
- be age and ability appropriate for the users and be suitable for educational settings.
- handle multilingual web content, images, common misspellings and abbreviations.
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.
- provide alerts when any web content has been blocked
- aim to provide enhanced/differentiated user-level filtering

A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

### 8.2 Monitoring

Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows you to review user activity on school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

The monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users

- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

### 8.3 Filtering and Monitoring Responsibilities

DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include:

Role	Responsibility
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.
Senior Leadership	Team Member Responsible for ensuring these standards are met and: <ul style="list-style-type: none"> <li>• procuring filtering and monitoring systems</li> <li>• documenting decisions on what is blocked or allowed and why</li> <li>• reviewing the effectiveness of your provision</li> <li>• overseeing reports</li> </ul> Ensure that all staff: <ul style="list-style-type: none"> <li>• understand their role</li> <li>• are appropriately trained</li> <li>• follow policies, processes and procedures</li> <li>• act on reports and concerns</li> </ul>
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: <ul style="list-style-type: none"> <li>• filtering and monitoring reports</li> <li>• safeguarding concerns</li> <li>• checks to filtering and monitoring systems</li> </ul>
IT Service Provider	Technical responsibility for: <ul style="list-style-type: none"> <li>• maintaining filtering and monitoring systems</li> <li>• providing filtering and monitoring reports</li> <li>• completing actions following concerns or checks to systems</li> </ul>
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	<ul style="list-style-type: none"> <li>• they witness or suspect unsuitable material has been accessed</li> <li>• they can access unsuitable material</li> <li>• they are teaching topics which could create unusual activity on the filtering logs</li> <li>• there is failure in the software or abuse of the system</li> <li>• there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks</li> <li>• they notice abbreviations or misspellings that allow access to restricted material</li> </ul>

### 8.4 Changes to Filtering and Monitoring Systems

There should be a clear process for requests to change the filtering and monitoring systems and who makes the decision to alter the filtering system. Requests are made via a Google Form to the OSL and DSL detailing the reasons for and the duration of the change. The OSL will note on the sheet when the change is made and when filtering reverts back to normal.

### 8.5 Filtering and Monitoring Review and Checks

To understand and evaluate the changing needs and potential risks of the school, the filtering and monitoring provision will be reviewed at least annually. The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider. Additional checks to filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and meeting safeguarding obligations.

### **8.6 Reviewing the filtering and monitoring provision**

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff.

The review will take account of:

- the risk profile of learners, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of learners
- teaching requirements, for example, the RHSE and PSHE curriculum
- the specific use of chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies are in place
- what checks are currently taking place and how resulting actions are handled

To make the filtering and monitoring provision effective, the review will inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review will be carried out as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, e.g. remote access or BYOD
- new technology is introduced

### **8.7 Checking the filtering and monitoring systems**

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on a range of:

- school owned devices and services, including those used off site
- geographical areas across the site

- user groups, for example, teachers, pupils and guests

Logs of checks are kept so they can be reviewed. These record:

- when the checks took place
- who did the check
- what was tested or checked
- resulting actions

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed:

[SWGfL Test Filtering](#)

### **8.8 Training/Awareness:**

It is a statutory requirement in England that staff receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring. Furthermore, in order to protect personal and sensitive data, governors, senior leaders, staff and learners should receive training about information security and data protection, at least annually.

Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring (Responsible Governor, DSL, OSL or other relevant persons) will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:

- in lessons
- through the acceptable use agreements

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc.

### **8.9 Audit**

Governors/SLT/DSL/OSL will ensure that full records are kept of:

- Training provided
- *Security incidents related to this policy*
- *Annual online safety reviews including filtering and monitoring*
- *Changes to the filtering system*
- *Checks on the filtering and monitoring systems*

## 8. Outcomes

The impact of the Cybersecurity and Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

## Appendix 1 Current filtering and monitoring provision

The school is currently using Smoothwall for filtering and monitoring, and based on the UK Safer Internet Centre audit, is therefore compliant with the required filtering and monitoring standards.

# Appropriate Monitoring for Schools



May 2023

## Monitoring Provider Checklist Responses

Schools (and registered childcare providers) in England and Wales are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering”. Furthermore, it expects that they “assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology”. There are a number of self review systems (eg [www.360safe.org.uk](http://www.360safe.org.uk)) that will support a school in assessing their wider online safety policy and practice.

The Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ obliges schools and colleges in England to “ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness” and they “should be doing all that they reasonably can to limit children’s exposure to [Content, Contact, Conduct, Contract] risks from the school’s or college’s IT system” however, schools will need to “be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

By completing all fields and returning to UK Safer Internet Centre ([enquiries@saferinternet.org.uk](mailto: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	Smoothwall (part of Qoria)
Address	Second Floor, 2 Whitehall Quay, Leeds, LS1 4HR
Contact details	<a href="https://www.smoothwall.com/education/contact-us/">https://www.smoothwall.com/education/contact-us/</a>
Monitoring System	Smoothwall Monitor
Date of assessment	30/08/2023

### System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

## Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
<ul style="list-style-type: none"> <li>Are IWF members</li> </ul>		Yes, Smoothwall is a member of the Internet Watch Foundation and implement the IWF CAIC list.
<ul style="list-style-type: none"> <li>Utilisation of IWF URL list for the attempted access of known child abuse images</li> </ul>		The images we see are generally screenshots, and as such aren't suitable for hashing. Hashing is able only to match images with minor changes, and as such cannot hope to match (eg.) an image and that image screenshot in a user's browser.
<ul style="list-style-type: none"> <li>Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'</li> </ul>		Smoothwall has worked with CITRU for many years across both filtering and monitoring
<ul style="list-style-type: none"> <li>Confirm that monitoring for illegal content cannot be disabled by the school</li> </ul>		It is not possible to fully disable monitoring without uninstalling the system

## 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		There are 3 themes that cover this requirement - a specific theme on Terrorism, a specific theme on CAI and an additional theme on Grooming. Monitor uses a detailed process to ensure that we alert Users to activity within these themes, without propagating any images that may have been shared.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		The "Bullying" theme includes both entirely online bullying, and references to physical world counterparts.

Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Smoothwall Monitor includes the detection of contact with monitored users for sexual purposes. Monitoring looks for signs of grooming and requests for sexual information or images. The "Oversharer" theme alerts in
			instances where a monitored user might be providing personal information online – their address, full name or phone number for example.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Bullying detection also includes monitoring of bigotry, hatred and discrimination.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Drug and substance abuse would be classified as "General Risk", or in some cases "Vulnerable User" where the individual is at risk of exposure or has been exposed to drugs
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		The "Terrorism/Extremism" theme is designed entirely for detection of terror and extremism content
Gambling	Enables gambling		Gambling would be classified as "General Risk", or in some cases "Vulnerable User"
Pornography	displays sexual acts or explicit images		"Sexual Content" alerts will provide alerts when monitored users attempt to access or discuss pornography. Smoothwall recommends this is used in conjunction with a good quality web filter
Self Harm	promotes or displays deliberate self harm		The "Vulnerable user" theme includes detection of various activities related to self harm.
Suicide	Suggest the user is considering suicide		As with Self Harm, suicidal ideation and discussion of or researching suicide related material is covered by the "Vulnerable User" theme. If a risk to life is suspected, the DSL will receive a phone call straight away – 24/7/365.

Violence	Displays or promotes the use of physical force intended to hurt or kill		Violent material is covered by the Violence theme
----------	---	--	---

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

Smoothwall Monitor is powered by a combination of AI and human moderation. The moderation team sees data from many sources, so new trends are picked up rapidly. AI is excellent at spotting unusual trends, and outlier data, providing comprehensive coverage. With human feedback into the AI, the system is constantly learning and improving

## Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> <li>Age appropriate – includes the ability to implement variable monitoring appropriate to age and vulnerability. This will in turn define which alerts are prioritised and responded to. Further situations may warrant additional capability, for examples boarding schools or community based access</li> </ul>		Monitor has several age group settings which are applied during onboarding. This alters alert thresholds and settings relevant to the age group chosen. Age group settings can be applied to specific Groups of users, allowing for granular control of Monitoring sensitivity.
<ul style="list-style-type: none"> <li>Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided</li> </ul>		Monitor allows fully customisable alert settings for the site or groups within the site. Alerts can be tailored for each Safeguarding user of the system, allowing them to chose the Groups they receive alerts for, and the severity at which they will be notified.
<ul style="list-style-type: none"> <li>Audit – Any changes to the monitoring system are logged enabling an audit trail that ensures transparency and that individuals are not able to make unilateral changes.</li> </ul>		Users are not able to perform any actions in the UI that would cause concern. For example they are not able to delete alerts from the database.

<ul style="list-style-type: none"> <li>● 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</li> </ul>		<p>Monitor does not currently fully cater for BYOD. However if a student logs into their school Chrome account on a BYOD that activity would be Monitored.</p>
<ul style="list-style-type: none"> <li>● Data retention –what data is stored, where is it (physically– ie cloud/school infrastructure) stored and for how long. This should also include any data backup provision</li> </ul>		<p>Data is stored on our secure servers for a period of 15 months and then permanently deleted. Monitor's integration with all widely-used</p>
		<p>safeguarding record keeping systems allows Safeguarding users to automatically copy data across, providing longer term storage</p>
<ul style="list-style-type: none"> <li>● Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers</li> </ul>		<p>Monitor supports Windows, MacOS, iOS and ChromeOS. Customers are informed of this during the sales and onboarding process.</p>
<ul style="list-style-type: none"> <li>● Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy</li> </ul>		<p>Schools have the option to feed back into the moderation system, however we do not permit individual words to generate an alert – this would usually result in many more alerts. The AI and human moderation components are part of a carefully calibrated system where new sources of alerts are added by our professional analysts.</p>
<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>		<p>Requirements for monitoring across all sites within a group of schools will be discussed during a customer's onboarding. Where centrally-managed policies are required they can be easily mirrored across sites, and central users can be given a variety of levels of visibility over their sites. Monitor's reporting tools are</p>

		suitable for single sites and large groups of schools, and automatically display information on all sites the user has access to.
<ul style="list-style-type: none"> <li>Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?</li> </ul>		Smoothwall provides assistance to customers in informing their users about monitoring with Smoothwall Monitor
<ul style="list-style-type: none"> <li>Multiple language support – the ability for the system to manage relevant languages?</li> </ul>		Smoothwall Monitor is used across the UK, US and Australia. Monitor fully supports English and Spanish, and contains a number of keywords from many commonly-used languages.
<ul style="list-style-type: none"> <li>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?</li> </ul>		Alerts are categorised on a scale of 1 to 5, initially by AI, then a human reviewer. Alerts are then sent according to theme and severity. Almost all events will trigger an email, some higher level events will trigger a phone call to the Safeguarding Team
<ul style="list-style-type: none"> <li>Remote monitoring – with many children and staff working remotely, the ability, extent and management for the monitoring of devices (school and/or personal). Included here is the hours of operation together with the explicit awareness of users.</li> </ul>		Monitored devices are actively monitored 24/7/365, whether the device is in-school or elsewhere. All activity on a monitored device will be analysed. Only school- issued devices and accounts are supported by Monitor. Smoothwall provides assistance to schools in making users and parents aware of monitoring.
<ul style="list-style-type: none"> <li>Reporting – how alerts are recorded within the system?</li> </ul>		Alerts are recorded separately to capture information. All alerts are available in the portal and can be searched, linked through to associated screen captures.

		Permanent storage should be in the school's record management system. A full set of reports over time showing alert types and levels is available within the Monitor dashboard.
<ul style="list-style-type: none"> <li>● Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)</li> </ul>		Images which accompany captures are reviewed by the moderation team.

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

Smoothwall monitor only supports pro-active monitoring. Smoothwall believes this is the only way monitoring implementations can be successful. Automation is used to support the monitoring team in weeding out captures which are not harmful, and presenting the moderation team with the data in the most efficient way. The moderation team are all Smoothwall employees, fully DBS checked, and have the support of counsellors and the HR team. None are on a zero hours contract. The moderation team do not make decisions on the outcome, they are there to make sure you don't see false positives. As such, they are not trained safeguarders per se, rather operatives trained in understanding what they are seeing and whether a DSL or other safeguarder would need to be alerted.

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

As part of the wider Qoria group, Smoothwall offers a huge range of products and support for schools, including best in class Monitoring, Record Management, Classroom Management and Student Wellbeing tools. Additionally Smoothwall offers training and resources to promote safety in UK schools, including a school branded "hub" for parents and students.

## 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	Tracy Harper
Position	Product Director - Early Detection and Intervention
Date	31/08/23
Signature	

# Filter Pyramid

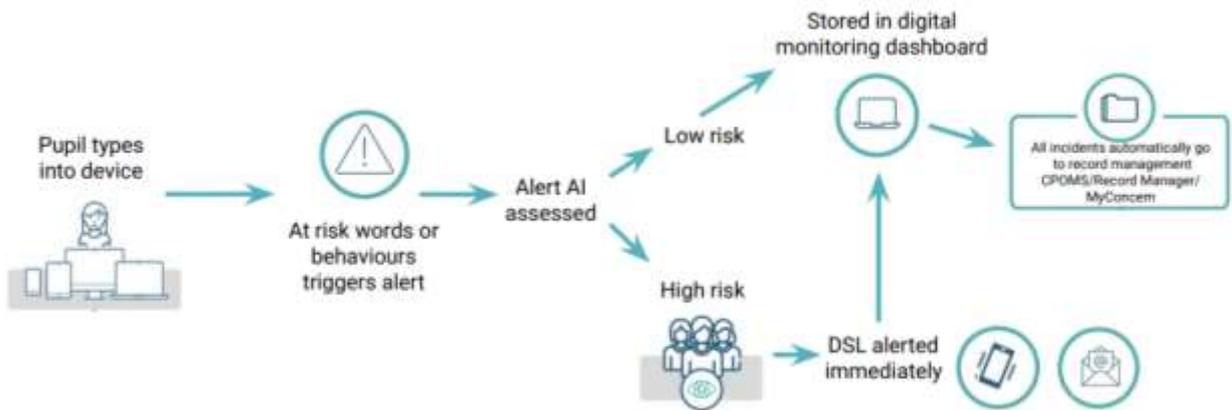
You want to be at the top



smoothwall.com



# Digital monitoring - how it works



smoothwall.com

