Belonging Believing Becoming

Thrive
CE Academy Trust

Online Safety Policy

19th September 2023

Contents

1. Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, local governors and trustees.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

- **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
- **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
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

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
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- 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.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Local Governing Board

The local governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The local 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.
The local governing board will also 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.
The local governing board will 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).

The local governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
The local governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The

board will 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 these standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure 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

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and DDSL are set out in each school's Child Protection Policy and Safeguarding Policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and local governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or local governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting full security checks and monitoring the school's ICT systems as outlined in appendix 7
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the Academy Trust Board immediately.
- Following the correct procedures by working closely with their ICT provider/manager if they need to bypass the filtering and monitoring systems for educational purposes but ensuring permission is granted by the DSL and Headteacher.

- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

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

3.7 Visitors and members of the community

Visitors 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 (appendix 3).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary school

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

All schools –

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

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.

6. Cyber-bullying

6.1 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.)

6.2 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. Teachers will discuss cyber-bullying with classes.

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 (see section 11 for more detail).

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.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher and DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Headteacher in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Thrive CE Academy Trust recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Thrive CE Academy Trust will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the any school within the Trust.

7. Acceptable use of the internet in school

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 (appendices 1 to 3). 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.

We 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.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the school's IT provider/manger and inform the Headteacher and DSL.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS.

This policy will be reviewed every year by the Trust Board. At every review, the policy will be shared with the local governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices

- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Ask a teacher or adult if I can do so before using them • Only use websites that a teacher or adult has told me or allowed me to use • Tell my teacher immediately if: ○ I select a website by mistake ○ I receive messages from people I don't know ○ I find anything that may upset or harm me or my friends • Use school computers for school work only • Be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password • Never share my password with anyone, including my friends • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer • Save my work on the school network • Check with my teacher before I print anything • Log off or shut down a computer when I have finished using it **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Signed (parent/carer):	**Date:**

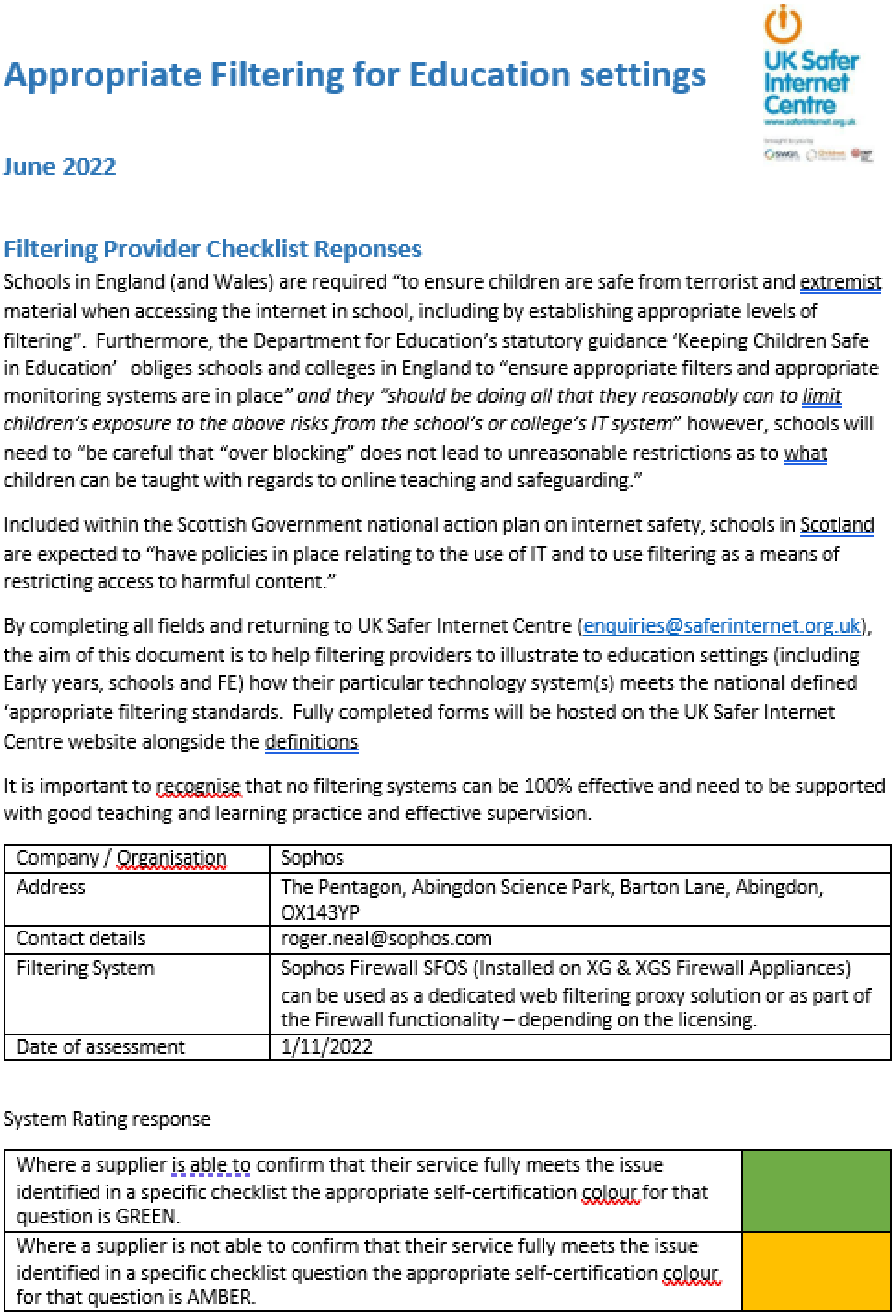
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: Filtering Provider Response – Didsbury CE, St. Wilfrid's, West Didsbury



Appropriate Filtering for Education settings

UK Safer Internet Centre
www.saferinternet.org.uk

June 2022

Filtering Provider Checklist Reponses

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), 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	Sophos
Address	The Pentagon, Abingdon Science Park, Barton Lane, Abingdon, OX143YP
Contact details	roger.neal@sophos.com
Filtering System	Sophos Firewall SFOS (Installed on XG & XGS Firewall Appliances) can be used as a dedicated web filtering proxy solution or as part of the Firewall functionality – depending on the licensing.
Date of assessment	1/11/2022

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
• Are IWF members	GREEN	Yes, Sophos is a member of the Internet Watch Foundation and routinely works with the IWF and other agencies in helping to identify the methods used by child abusers to share content, reporting the discovery of child abuse images online
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)	GREEN	Yes, Sophos actively implements the IWF CAIC list.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	GREEN	Yes, Sophos actively integrates 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.	GREEN	Sophos provides an "Intolerance and Hate" category to enable blocking of sites that foster racial supremacy or vilify/discriminate against groups or individuals. Sophos recommends blocking this category.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	GREEN	Sophos provides "Controlled Substances", "Marijuana" and "Legal Highs" categories that enable blocking of sites providing information about or promoting the use, trade or manufacture of drugs. Sophos recommends blocking these three categories.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	GREEN	Sophos provides an "Intolerance and Hate" category to enable blocking of sites that promotes terrorism and terrorist ideologies, violence or intolerance. Sophos recommends blocking this category.
Malware / Hacking	promotes the compromising of systems including anonymous	GREEN	Sophos provides "Anonymizers", "Hacking, Phishing and Fraud",

	browsing and other filter bypass tools as well as sites hosting malicious content		"Spam URLs" and "Spyware and Malware" categories. Sophos recommends blocking these categories. In addition, all unencrypted content is scanned for malware. A cloud-delivered sandbox analyses any downloaded active content and blocks malware.
Pornography	displays sexual acts or explicit images	GREEN	Sophos provides "Sexually Explicit", "Nudity" and "Extreme" categories. Sophos recommends blocking these categories. Also, Sophos provides "Safe-Search" enforcement on the major search engines. The option is also available to add a "Creative Commons" license that only shows images published under Creative Commons licensing laws. To date, using this method has not resulted in any pornographic images being forwarded to Sophos for reclassification.
Piracy and copyright theft	includes illegal provision of copyrighted material	GREEN	Sophos provides "Peer to peer and torrents" and "intellectual piracy" categories. Sophos recommends blocking these categories.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	GREEN	Sophos provides the "Pro-suicide and self-harm" category. Sophos recommends blocking this category.
Violence	Displays or promotes the use of physical force intended to hurt or kill	GREEN	Sophos provides "Extreme" and "Criminal Activity" categories. Sophos recommends blocking these categories to block sites displaying or promoting the use of physical force intended to hurt or kill.

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

Sophos currently provides 91 different URL categories. For the full list see: https://www.sophos.com/threat-center/reassessment-request/utm.aspx. Sophos Labs enables us to dynamically update our web categories by providing a URL categorisation services that integrate Sophos URL data with that of multiple third-party suppliers, including IWF and CTIRU, to provide a market-leading database. Sophos classifies sites at the IP level, domain, sub-domain and path URL data is constantly reviewed and unclassified websites are classified on an hourly basis via a cloud delivered service to the Sophos appliance (Physical, Virtual or in Public Cloud), so they are always up-to-date with the latest classifications for sites.

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 .

Sophos Firewall retain reports on box for up to a year. This is potentially impacted by disk space which is checked during the scoping phase with Sophos engineers. As the disk reaches its maximum capacity it will delete the eldest records. Therefore, if the box has additional work to do that wasn't covered in the scoping its possible that the retention phase is reduced. It is possible to choose to use Central Reporting which would give 30 days of reporting with an XGS Xstream license, with increased licensing blocks available for purchase to meet a schools retention needs or purchase additional data storage packs for longer storage on Sophos Central.

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

Sophos category database protects more than 400,000 organizations in more than 150 countries. The huge amount of data helps Sophos to fine tune our web filtering policies based on the typical activities of users in different settings. Sophos also provides tools that enable customers to create custom categories that over-ride current URL database classifications and end-users to request page reclassification, by the system administrator, directly from the block page. Education establishments can therefore tweak their web filtering policies to make sure they are enabling their staff and students to be the best and brightest they can be. Safe in the knowledge that they are also helping keep their users safe online.

Filtering System Features

How does the filtering system meet the following principles:

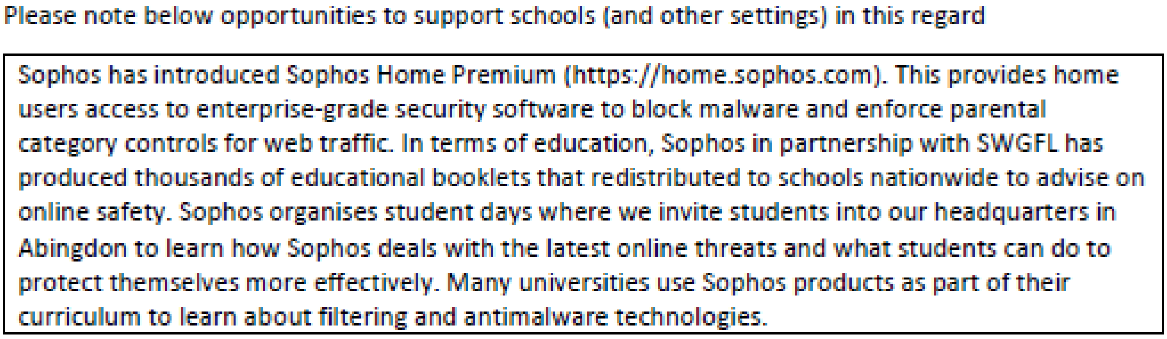
Principle	Rating	Explanation
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role	GREEN	Sophos can apply policy rules based on group information. If the school includes objects related to age then policies can be created that open certain categories of websites once a certain age has been reached (e.g. the "Sex Education" category. Sophos also logs all user group activity separately for reporting. Reports can be generated for a specific event in a specific user group. All alerts can be sent using syslog into a Security Incident and Event Management system (SIEM).
• Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy	GREEN	Sophos provides the "Anonymizers' category in our web filter. Sophos recommends blocking this category. Whilst we also provide a 'block filter avoidance app' application rule. Both policies would block users from being able to circumvent their filtering

services and DNS over HTTPS.		
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content	GREEN	The day-to-day administration of the Sophos Firewall appliance is done by the school IT team (or partner if this is out-sourced). There is complete flexibility in the policy model to create policies that can block categories, file types, URLs, IPs and much more. Policies can be created easily and intuitively using a very user-friendly interface.
• 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	GREEN	The Sophos Firewall includes a content scanning feature, whereby URLs and web pages are dynamically analysed for specific keywords or phrases. Customers can upload multiple keyword lists to support different languages and provide better granularity. Any pages matching words or phrases contained within the keyword lists can be blocked and/or logged. In addition, Administrators/Safeguarding officers can review the blocked keywords using the onboard log viewer and determine the context.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	GREEN	Sophos provides the rationale behind its web classification so that accurate choices can be made by IT administrators. This information can be found here: https://support.sophos.com/support/s/article/KB-000036518?language=en_US
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	GREEN	Sophos provides a central management console that enables you to manage multiple site based (MAT for example) Firewalls in one console. Central policy can be configured and pushed out to your different sites. Whilst reporting and alerting can all be managed centrally
• Identification - the filtering system should have the ability to identify users	GREEN	Sophos Firewall can identify users transparently via Single-Sign on or through integration with directory server login processes or via the Sophos Endpoint Protection Client. It can also provide non-transparent authentication where a user is required to login before browsing.
• 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	GREEN	Sophos Firewall is able to filter all http and https connections including TLS 1.3 encrypted traffic. This is not limited to browser traffic and includes mobile and app connections. Sophos also provides policy-driven application control that can also identify and manage traffic that uses other protocols

technologies (beyond typical web browser delivered content)		
• Multiple language support – the ability for the system to manage relevant languages	GREEN	Sophos Firewall supports multiple block pages to support multiple languages and custom block pages where multiple languages are required on the same page.
• 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)	GREEN	Sophos Firewall can be deployed as a standalone web proxy or in transparent bridge or gateway mode
• 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	GREEN	For Windows and Mac devices that are not on the school network, web filtering can be enforced using our Sophos Central Endpoint protection client. This includes web control, which has specific policies for remote devices. These policies can be managed via Sophos Central (our Cloud management platform) and any violations can be reported on. There are over 48 categories that can be configured, as well as file type blocking. This includes sites that are on the IWF and Counter Terrorism Referral Unit block lists. Webfiltering on Chromebooks can also be controlled via Sophos Mobile (UEM Solution).
• Reporting mechanism – the ability to report inappropriate content for access or blocking	GREEN	Sophos provides a number of built-in reports that can be used to see this information. These reports are fully customisable and can be emailed to admins/teachers/safeguarding officers. In addition, the log files can be exported using syslog to third party tools.
• Reports – the system offers clear historical information on the websites visited by your users	GREEN	Sophos provides a number of built-in reports that can be used to see this information. In addition the log files can be exported using syslog to third party tools.

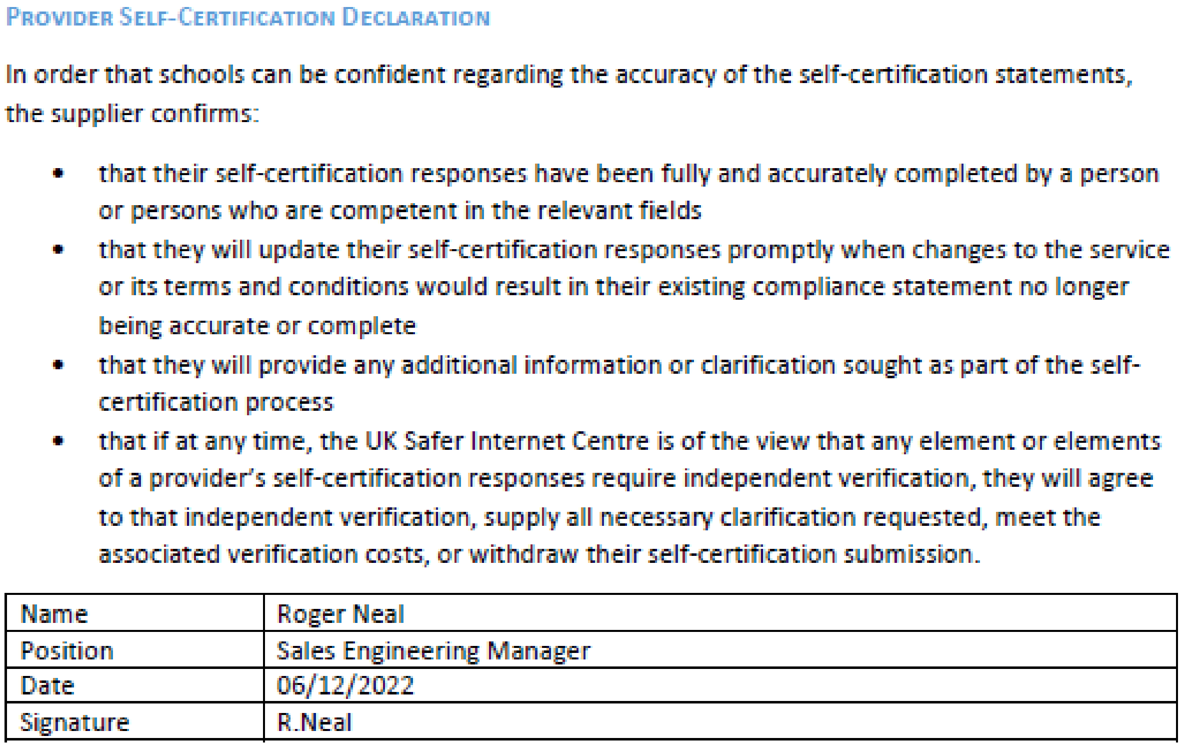
Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to *"consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum"*.[1]

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2



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

Sophos has introduced Sophos Home Premium (https://home.sophos.com). This provides home users access to enterprise-grade security software to block malware and enforce parental category controls for web traffic. In terms of education, Sophos in partnership with SWGFL has produced thousands of educational booklets that redistributed to schools nationwide to advise on online safety. Sophos organises student days where we invite students into our headquarters in Abingdon to learn how Sophos deals with the latest online threats and what students can do to protect themselves more effectively. Many universities use Sophos products as part of their curriculum to learn about filtering and antimalware technologies.



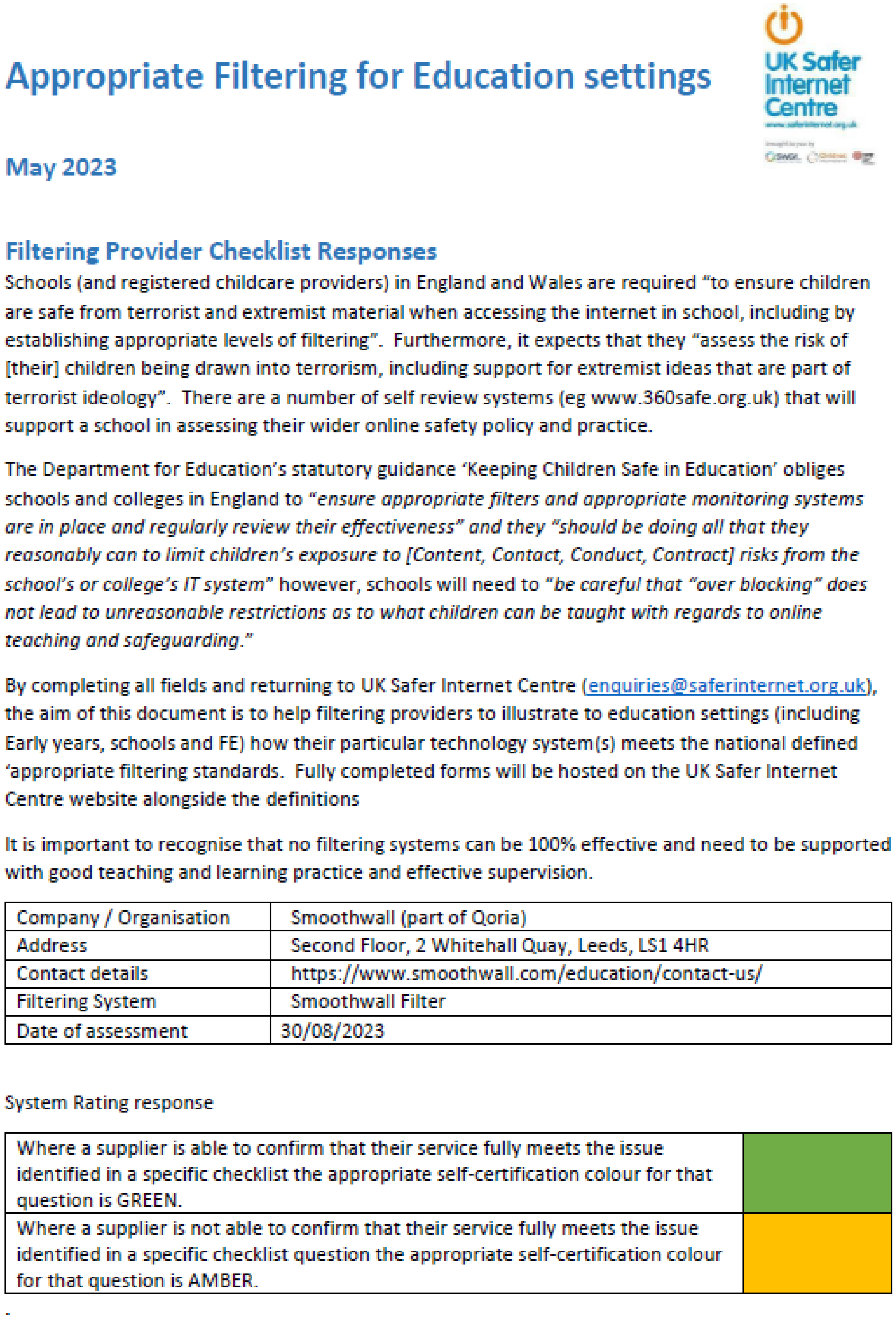
Provider Self-Certification Declaration

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	Roger Neal
Position	Sales Engineering Manager
Date	06/12/2022
Signature	R.Neal

Appendix 6: Filtering Provider Response – St. Elisabeth's



Appropriate Filtering for Education settings

May 2023

Filtering 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) 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), 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 (part of Qoria)
Address	Second Floor, 2 Whitehall Quay, Leeds, LS1 4HR
Contact details	https://www.smoothwall.com/education/contact-us/
Filtering System	Smoothwall Filter
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.	🟨

-

Illegal Online Content

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

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.
• Confirm that filters for illegal content cannot be disabled by the school	🟩	It is not possible to disable the illegal content filter rules

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.
Gambling	Enables gambling	🟩	The Gambling category includes all online gambling sites, along with sites promoting gambling or discussing strategies for gambling
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 has an in-house Digital Safety Team which is 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
• Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff	🟩	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. It is also possible to combine user group with location (eg outside school)
• 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.	🟩	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. Agent based filtering adds an additional layer of protection.
• Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content.	🟩	Smoothwall Filter has a full range of policy tools available, allowing School

Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes	🟩	users to easily make policy changes, test a site against current policy or simply quickly allow or block a site.
• 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, this would include AI generated content. For example, being able to contextually analyse text on a page and dynamically filter.	🟩	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.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	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.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	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.
• Identification - the filtering system should have the ability to identify users	🟩	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.
• 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). Providers should be clear about the capacity of their filtering system to manage content on mobile and web apps	🟩	Any app content delivered via HTTPS (not necessarily through a web browser) can be blocked and inspected by Smoothwall’s on-premise network appliance, assuming the app permits this. In addition, Smoothwall’s optional firewall module can

	🟩	identify and block many other types of app.
- Multiple language support – the ability for the system to manage relevant languages	🟩	Smoothwall's combined blocklist includes 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.
- 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)	🟩	Smoothwall Filter offers both network level filtering, and device based filtering, for use as appropriate.
- Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school	🟩	Smoothwall's Cloud Filter provides identical filtering capabilities to the on-premise system including dynamic, contextual real-time content filtering.
- Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	Smoothwall provides the ability to report overblocked content to the administrator. Uncategorised content (which is possibly "underblocked") is automatically fed back to Smoothwall and will subsequently be appropriately categorised.
- Reports – the system offers clear historical information on the websites users have accessed or attempted to access	🟩	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.
- Safe Search – the ability to enforce 'safe search' when using search engines	🟩	Smoothwall offers forced safesearch on all major search engines, social media sites and some niche providers.

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”*.[1]

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

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.

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	VP Product
Date	30/08/2023
Signature	

Appendix 7: Academy Filtering and Monitoring Procedures

Filtering

Didsbury CE, St. Wilfrid's CE, West Disbury CE

I.T Provider: One Education IT
Filtering Software: Sophos
Overview:
Weekly report generated and sent to Headteacher/DSL. This report will identify

1. Blocked Web Users
2. Blocked Web Categories
3. Blocked Web Domains
4. Blocked Web Hosts
5. Blocked Web Applications
6. Blocked Allowable Categories
7. Blocked Allowable Domains
8. Blocked Policies

These reports will identify the time and specific machine which has tried to access content.

St. Elisabeth's CE
I.T. Provider: AVA Stockport
Filtering Software: Smoothwall
Overview:

1. Checks take place in real time, first by AI filtering and then passed to a member of AVA team for consideration.
2. School contacted (phone) once risk identified with details of the user/machine and time accessed.
3. Details entered into online log which is accessible by the Headteacher.

Monitoring

All Schools
Monitoring Type: Physical Monitoring
Log-on Details: Group/Generic
Overview:
Each piece of equipment which can be used to access the internet is numbered. Pupils are encouraged to use the same equipment whenever possible, and logs are kept of the device number used by a pupil at any given time. These monitoring logs are checked regularly by the Headteacher/DSL to ensure compliance with the policy. Currently school devices are not used away from the school.

Reporting

All schools will adhere to this policy and ensure that staff have up to date training regarding internet safety, filtering and monitoring. All concerns will be dealt with inline with the relevant safeguarding policy or code of conduct policy for staff. CPOMS will be used to record all safeguarding concerns, including those linked to internet safety.