



**Ivington C of E  
Primary and  
Pre-school**

*Reaching together with the Fruit of the  
Spirit (Galatians 5:22-23)*

**Filtering and Monitoring Policy**

# Approval of the Governing Body

This document is a statement of the aims, principles and strategies for:

## **Filtering and Monitoring**

at

## **Ivington CE (VA) Primary and Pre-school**

It was revised during the:

**Summer Term 2024**

It has been agreed and is supported by the teaching staff and the governing body

We aim to review this policy during the:

**Summer Term 2026**

Or sooner if necessary



## **Linking with our Vision – Reaching together with Love, Joy and Peace (Galatians 5:22-23)**

**To provide a caring, Christian ethos for the school, which inspires and excites a shared enthusiasm for life and learning.**

At Ivington CE Primary and Pre-school, through our strong Christian ethos and focus on nine important Christian values, we are committed to providing a deeply nourishing, spiritual, ambitious, and broad curriculum.

Our motto, 'Reaching together' underpins our belief in equality of opportunity for all, where we actively endeavour to promote understanding and appreciation of our diverse society and give each child a special place in the world where they feel valued, essential to our community and equipped with the necessary skills to make a positive contribution.

We perceive our role to be opening a 'Window on the World', through which our pupils are actively encouraged to develop respect for the beliefs and cultures which enrich their everyday lives and encourage others to do likewise.

We strive to eliminate inequality through our deep Christian ethos of respect and understanding of all groups in society, which ensures that everyone at Ivington will be treated fairly despite his or her creed, colour, disability, or gender.

More details are available in our Inclusion, Racial Equality and Equal Opportunities policies.

The health, safety, and welfare of all the people who work or learn at our school are therefore of fundamental importance. We aim to provide a safe, secure, and pleasant working environment for everyone. The governing body, along with the LA, takes responsibility for protecting the health, safety and welfare of all children and members of staff.

## Policy Links

This policy links to the following other policies:

- **Safeguarding and Child Protection Policy**
- **E Security Policy**
- **E Safety Policy**

## Ready, Respectful, Safe

At Ivington, we are committed to creating an environment where outstanding behaviour is at the heart of everything we do. Everyone is expected to maintain the highest standards of personal conduct, to accept responsibility for their behaviour and encourage others to do the same. We aim to be calm and consistent at all times in our dealing with children; this fits with the calm, quiet and productive working environment we aim to foster.

Restorative practice is key to our approach and there is an expectation that everyone develops trusting communication with one another. This includes all staff, children, visitors, parents and carers.

We want our learners to be '**Ready**' to learn, to be '**Respectful**' of each other and to feel '**Safe**'. We want this relationships policy to echo this.

## Filtering and monitoring: review template

Reviewing your system means to scrutinise whether it's still the right one for your school.

If you already use a tool to audit your approach to online safety and/or cyber security, check to see if it covers filtering and monitoring. If you're not sure, reach out to your IT service provider.

If it doesn't, use our template below alongside your wider online safety/cyber security review processes.

Review your filtering and monitoring provision **annually**, or where:

- You identify a safeguarding risk
- There's a change in your working practice (e.g. you allow remote access or staff to bring their own device)
- You introduce new technology

Use your filtering and monitoring review to inform:

- Your school's related safeguarding or technology policies and procedures
- Roles and responsibilities
- Staff training
- Curriculum and learning opportunities
- Procurement decisions
- What is checked, and how often
- Monitoring strategies

4 things you need to do to have effective filtering and monitoring

You need to:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems
- Block harmful and inappropriate content without unreasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet your safeguarding needs
- Review filtering and monitoring provision at least annually

## ROLES AND RESPONSIBILITIES

Day to Day Management (DSL and IT service provider)	<ul style="list-style-type: none"> <li>• Procure systems</li> <li>• Identify risk</li> <li>• Carry out reviews</li> <li>• Carry out checks</li> </ul>	Headteacher John Finch Computers
Day to Day Management (DSL)	<ul style="list-style-type: none"> <li>• Filtering and Monitoring Reports</li> <li>• Safeguarding Concerns</li> <li>• Checks and filtering to monitoring system</li> </ul>	DSL, DDSLs, Headteacher <a href="mailto:securlyalerts@ivington.hereford.sch.uk">securlyalerts@ivington.hereford.sch.uk</a> monitored by M Smith, R Thompson, N Rogers
Day to Day Management (IT service provider - John Finch Computers)	<ul style="list-style-type: none"> <li>• Maintaining the filtering and monitoring system</li> <li>• Providing filtering and monitoring reports</li> <li>• Checking the system or completing actions following any concerns</li> </ul>	John Finch Computers
Day to Day Management (SLT)	<ul style="list-style-type: none"> <li>• Buying-in the filtering and monitoring system the school use</li> <li>• Documenting what is blocked or allowed, and why</li> <li>• Reviewing the effectiveness of provision, making sure that incidents are urgently picked up, acted on and outcomes are recorded</li> <li>• Overseeing reports</li> <li>• Making sure staff: <ul style="list-style-type: none"> <li>○ Understand their role</li> <li>○ Are trained appropriately</li> <li>○ Follow policies, processes and procedures</li> <li>○ Act on reports and concerns</li> </ul> </li> </ul>	Headteacher, Deputy Headteacher/computing lead

## ROLES AND RESPONSIBILITIES

Day to Day Management (all staff)	<p>Everyone should be clear on:</p> <ul style="list-style-type: none"> <li>The expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of their safeguarding training. For example, part of their role may be to monitor what's on pupils' screens</li> <li>How to report safeguarding and technical concerns, such as if: <ul style="list-style-type: none"> <li>They witness or suspect unsuitable material has been accessed</li> <li>They are able to access unsuitable material</li> <li>They are teaching topics that could create unusual activity on the filtering logs</li> <li>There is a failure in the software or an 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> </li> </ul>	All teaching staff, teaching assistants, wrap around care staff and lunch supervisors
Day to Day Management (Governing Board)	<p>Has overall strategic responsibility for filtering and monitoring.</p> <p>They will need assurance from you that your school is meeting the standards and they need to be aware of what's going on</p>	<p>Governing body</p> <p>Safeguarding governor</p> <p>Vulnerable groups governor</p>

REVIEW TEMPLATE	ANSWER	NEXT STEPS/ACTIONS
If you're part of a multi-academy trust (MAT): is the level of online protection the same across all schools in the MAT?	N/A	

REVIEW TEMPLATE	ANSWER	NEXT STEPS/ACTIONS
<p>What is the risk profile of your pupils? E.g:</p> <ul style="list-style-type: none"> <li>○ Their age range</li> <li>○ Pupils with special educational needs and disabilities (SEND)</li> <li>○ Pupils with English as an additional language (EAL)</li> </ul>	<p>We have a high proportion of children with SEND, some of these children use tablets and laptops more than other children to access their learning.</p>	<ul style="list-style-type: none"> <li>• Termly checks on pupil tablets to make sure filtering systems are still in place and effective</li> <li>• Procure a monitoring system that allows teachers to view tablet screens for all pupils during a lesson</li> </ul> <p>Is this something we could use?</p> <p>This happens automatically</p> <p>Updates and reboots happen at the end of the half terms. John Finch Computers checks all running correctly</p>
<p>Does your filtering and monitoring system adhere to the technical requirements? (get your checklist of the requirements <a href="#">here</a>)</p>	<p>See below</p>	



REVIEW TEMPLATE	ANSWER	NEXT STEPS/ACTIONS
What does your filtering system currently block or allow, and why?	<p>Our school's Internet connection is filtered by a product called <b>Securly</b> and it can be found at <a href="http://www.securly.com">www.securly.com</a>. It is a fully cloud-based filtering service so requires no additional hardware located at the school site or software installed onto devices. It operates at network level across all hardware. It is multi-lingual and also filters encrypted (https) traffic.</p> <p>Securly has been a member of the Internet Watch Foundation since 1<sup>st</sup> March 2016 and is a member of the Counter-Terrorism Internet Referral Unit list.</p> <p>Securly, by default, blocks access to the following content.</p> <ul style="list-style-type: none"> <li>• Discrimination</li> <li>• Drugs/Substance abuse</li> <li>• Extremism</li> <li>• Gambling</li> <li>• Malware/Hacking</li> <li>• Pornography</li> <li>• Piracy and Copyright Theft</li> <li>• Self Harm</li> <li>• Weapons and Violence</li> </ul> <p>Securly filters all traffic that uses the school's Internet connection. All attached devices including guest/BYOD devices connected to the schools wifi, apart from those logged into by staff members, are filtered at the same level of filtering as pupils. Staff members are filtered at a different level appropriate to their work.</p> <p>Securly will automatically send alerts to a separate school email mailbox which designated staff members have access to. Designated school staff are able to monitor alerts 24/7 if required. The alert message contains information regarding the block and identifying who did this, what the block entailed as well as the date and time. Designated school staff have access to the Securly portal to investigate the block further</p>	

REVIEW TEMPLATE	ANSWER	NEXT STEPS/ACTIONS
<p>What limitations are there to your filtering system?</p> <p>How will you mitigate them?</p>	Continuing rapid development of APPs and new harmful terminology and technology	Keep staff and parents up to date with changes to online safety using the National Online Safety #WakeUpWednesday
<p>How do you know your filtering and monitoring system meets the needs of your school?</p> <p>(Use your Prevent risk assessment to help you decide what's appropriate for your school)</p>	<p>Recommended by our IT service– see Securly info above.</p> <p>John Finch Computers reviews all policies in April every year before renewing. If they are no longer meeting the needs of the schools, alternative provision is made.</p>	
<p>What outside safeguarding influences impact your school? E.g. county lines</p>	<p>County Lines</p> <p>Rural area encourages more online communication amongst pupils.</p>	
<p>Are there any relevant safeguarding reports that impact your filtering and monitoring?</p>	Older sibling of a child in the school accessing inappropriate material.	Monitor that this isn't influencing younger child. (Children's Services are involved.)
<p>What is the digital resilience of your pupils?</p> <ul style="list-style-type: none"> <li>• This means whether your pupils have the knowledge and skills to make decisions online that keep themselves safe, and whether they know what to do if they come across something that's wrong</li> </ul>	e-safety curriculum is revisited throughout each term. There are specific e-safety focus weeks in school in November and January.	<p>Pupil Voice at beginning of December and February</p> <p>Computing lead to monitor e-safety curriculum</p>
<p>Are you clear on your teaching requirements, for example, your RHSE and PSHE curriculum?</p>	<p>Teach Computing implemented Autumn 2023</p> <p>PSHE curriculum revised and implemented Autumn 2023 (Jigsaw)</p>	Subject leads for PSHE and Computing to monitor
<p>Does your school outline any specific uses of technologies? E.g. do you allow staff and/or pupils to 'Bring Your Own Device' (BYOD)?</p>	<p>See Acceptable Use Policy</p> <p>Children not allowed to bring devices apart from phones for older children which must be given to an adult.</p>	

REVIEW TEMPLATE	ANSWER	NEXT STEPS/ACTIONS
What related safeguarding or technology policies do you have in place?	Prevent Safeguarding Policy E-safety Policy GDPR	
What checks are currently taking place?  How do you handle any resulting actions?	Securely monitoring  HT follows up with update to staff, assembly information to pupils (in an age appropriate way) and immediate action	

## Filtering and monitoring: checks template

You need to carry out physical checks on your systems to make sure they're properly configured and that they haven't been changed or deactivated.

It's likely your IT service provider will carry out these checks in practice, but you still need to work with them and oversee the checks they're doing.

Do these checks termly, but you may decide to do them more often based on:

- Your context
- The risks highlighted in your review (above)
- Any other risk assessments

Your checks should cover a range of:

- School-owned devices and services, including those used off site
- Geographical areas across the site
- User groups, e.g. teachers, pupils and guests

CHECKS TEMPLATE	DATE OF CHECK	WHO DID THE CHECK	RESULTING ACTIONS
Have we checked that our filtering and monitoring system is still fit for purpose?  You can signpost your IT service provider to South West Grid for Learning's (SWGfL) <a href="#">testing tool</a> .	08/05/2024	John Finch Computers	Follow up meeting with HT July 2024

CHECKS TEMPLATE	DATE OF CHECK	WHO DID THE CHECK	RESULTING ACTIONS
Is the system running and working?	Yes 08/05/2024	John Finch Computers	Monitor at the end of each term
Have we checked that our filtering and monitoring system works on: <ul style="list-style-type: none"> <li>All devices</li> <li>New devices and services before they're given to staff or pupils</li> </ul>	Yes, this is carried out by John Finch Computers  28/02/2024	John Finch Computers	
Have we reviewed the list of blocked sites on our network?  Is this list still accurate/does it reflect any changes to safeguarding risks?	Blocked sites include: Manually blocked Coolmath.co.uk blocked 16th October 2023 Securly also blocks sites are on the website eg top blocked sites	John Finch Computers	Children not able to access site that advertised violent games
Does our filtering system adhere to the requirements?  (Get your checklist of the requirements <a href="#">here</a> )	Yes 08/05/2024	John Finch Computers	
Does our monitoring system adhere to the requirements?  (Get your checklist of the requirements <a href="#">here</a> )	Yes 08/05/2024	John Finch Computers	

## Monitoring strategy

Once you've reviewed your filtering and monitoring systems, make sure you've got the right monitoring strategy in place for your school (i.e. how monitoring will actually work in practice).

To choose your approach, use:

- Your review of your filtering and monitoring systems above
- Your [Prevent risk assessment](#)

- Any other relevant risk assessments or circumstances

We've outlined some different approaches you could take below.

Make sure you update all relevant policies to reflect your approach.

APPROACH	POINTS TO CONSIDER
<p>Physical monitoring</p> <p>(Where staff monitor pupils' screens while they're using them)</p>	<p>Use this approach where:</p> <ul style="list-style-type: none"> <li>• Your risk assessment(s) suggests <b>low risk</b></li> <li>• You have staff who can directly supervise pupils 1-to-1 whilst using technology</li> </ul> <p>Consider that:</p> <ul style="list-style-type: none"> <li>• It's difficult to physically monitor any independent use of technology</li> <li>• It can be resource intensive</li> <li>• It is less effective across a larger group, or a group using mobile devices</li> <li>• Students often adapt screen behaviour to avoid monitoring</li> <li>• Some devices cannot be monitored using any other strategy other than physical monitoring, e.g. taking videos/images on mobile devices or cloud storage</li> </ul> <p>But it is easier to intervene immediately where an issue arises, and you can use it as a teaching opportunity in the moment.</p>
<p>Internet and web access</p> <p>(Where schools can identify and intervene where someone has accessed or searched for something concerning.</p> <p>This is done by monitoring logfile information, which shows which individuals have accessed certain sites or used certain search terms)</p>	<p>Consider:</p> <ul style="list-style-type: none"> <li>• That you'll need to assign someone with the responsibility to analyse the logfile information <ul style="list-style-type: none"> <li>○ This will require time and specialist technical and/or safeguarding knowledge to analyse, as these reports can be difficult to understand</li> </ul> </li> <li>• How frequently these logfiles are updated by your provider</li> <li>• How you can regularly review these logfiles, analyse them and prioritise any alerts</li> <li>• That your logfile information needs to be able to identify individual users so you can intervene</li> <li>• That you must act on any information that indicates potential harm</li> <li>• How you retain logfile information. You need to make sure your data retention policies and logfiles include how long you'll retain this data</li> </ul>

APPROACH	POINTS TO CONSIDER
<p>Active/Pro-active technology monitoring services</p> <p>(These specialist services provide technology-based monitoring systems that actively monitor use across devices, through things such as keywords)</p>	<p>Use this approach where your risk assessment(s) suggests <b>high risk</b>.</p> <p><b>Active monitoring</b></p> <p>Where the system generates alerts for you to act on. This is effective where:</p> <ul style="list-style-type: none"> <li>You have enough capability and capacity to interrogate and interpret the volumes of information and alerts generated by the system</li> <li>You can assign appropriate safeguarding expertise to review, prioritise and take action on alerts</li> </ul> <p><b>Pro-active monitoring</b></p> <p>Where a third-party provider manages or supports alerts and may offer support with intervention. This is effective where you have a high number of devices operating.</p> <p>This system means:</p> <ul style="list-style-type: none"> <li>Your safeguarding staff are actively and immediately alerted to genuine risk threats to health or life</li> <li>You have a specialist organisation to provide additional capability and capacity to support your safeguarding staff</li> </ul> <p>Make sure you know whether your provider uses automation and what their team's safeguarding capability is.</p>

## Questions you can ask a new filtering and monitoring provider

If you need to decide on a new filtering and monitoring provider, cover the key areas with our questions below.

QUESTION	WHAT TO LOOK OUT FOR	NOTES
Does your filtering and monitoring system adhere to the technical requirements? (get your checklist of the requirements <a href="#">here</a> )	The provider needs to be compliant and adhere to best practice.	Yes
Does the provider work in, and align with, the education sector?	Some providers may not work with schools normally, so they may be unable to offer suitable support.	Yes

QUESTION	WHAT TO LOOK OUT FOR	NOTES
Is the provider based in the UK?	If you're looking at an international provider, be aware that their system may be geared more towards safeguarding issues that are less prominent in the UK. E.g. if you've selected a US provider, it may have a focus on school shooting content and may not adhere to requirements under the Prevent duty.	Yes
Can the provider give you school/education-specific case studies?	You want to see that the provider understands how to support schools and has a track record of doing this well.	Yes on the website
Can the provider give you a couple of school success stories with its system? What has been the impact of its product?	The provider should be able to explain how often they pick up a safeguarding alert or give an example of how their system helped to protect a child.	High uptake of schools using the system
Will the filtering and monitoring system work across all your devices?	Remember that the system needs to work on everything your school uses, from iPads to Chromebooks.	Yes
What technique does the provider use to filter websites?	This is to check how the provider categorises content and what the filter will see (you need to know how granular the filter is to decide if it's right for your school - will the filter only pick up domains or will it also pick up search terms?)	John Finch Computers will email Securly to confirm AI keyword matching, domain matching.
Does the provider offer granular or flexible filtering?	Some content you'll want to block for some year groups, but not others. Check to see if the provider gives you this option. This can help you to tackle 'over-blocking'. If you're in a multi-academy trust (MAT): make sure any sites you unblock are only unblocked for that specific school, and aren't automatically unblocked for all schools within the MAT	Granular e.g. coolmath.co.uk we have blocked by school Filtering happens automatically by Securly
Does the filtering and monitoring system identify individual users?	You need the provider to be able to flag which users have been searching for specific content so you can intervene (a general IP address alone is not helpful).	Yes

QUESTION	WHAT TO LOOK OUT FOR	NOTES
How will the provider monitor and how will it alert your school to concerns?	<p>Some providers will triage any problems first before alerting your school to cases of genuine concern, while others will ping an alert to you whenever a pupil searches for something deemed as concerning.</p> <p>Bear in mind:</p> <ul style="list-style-type: none"> <li>• What capacity your school has to deal with alerts that come in. All alerts need to be taken seriously by the DSL, so be sure they have the time they need</li> <li>• That alerts need to be looked at by someone with safeguarding training and experience (for example, a child searching for 'Mia' may look like a pupil searching for a friend's name, when in reality this is an acronym for pro-bulimia content)</li> </ul>	Emails to headteacher and deputy headteacher (computing lead)



## Blocked sites log

WEBSITE NAME AND URL	WHY IT'S BLOCKED	DATE BLOCKED	DATE UNBLOCKED (IF APPLICABLE)
Coolmath.co.uk	Advertising and easy access to games with violence as well as maths games	16 <sup>th</sup> October 2023	

## Staff request form template to unblock a specific website(s)

- Follow your school procedures to request a site be unblocked (for example, this might be through sending an email or submitting an IT ticket)
- Use our template below to help you structure your request

Staff name and year group/department:

Website title and URL/link:

Year group you want the website unblocked for (if applicable):

Reason why you want the website unblocked:

*E.g. students need to access it for classwork, homework, revision*

Can we re-block this site after a specific date?

No ☐

Yes ☐

Date the website can be re-blocked: \_\_\_\_\_

## Sources

- [Filtering and monitoring standards for schools and colleges](#) - the Department for Education (DfE)
- [Establishing appropriate levels of filtering](#) - the UK Safer Internet Centre
- [Appropriate monitoring: guide for education settings and filtering providers](#) - the UK Safer Internet Centre
- Luke Godfrey is UK marketing director at [Smoothwall](#), part of Qoria. Luke has a wealth of experience in the tech sector and has a real passion for protecting students online, enabling them to thrive in their digital lives
- Gareth Harle is an IT director who has worked managing and developing IT systems in education for almost 15 years across primary, secondary and FE sectors. His current role involves strategic planning and IT management across a multi-academy trust in Yorkshire
- Sian Stockham is deputy headteacher at King Ecgbert School in Sheffield. As an experienced senior leader, she has been involved in the leadership of safeguarding, online safety and IT strategy for well over a decade, and is passionate about the development of digital literacy and resilience in young people
- Kat Howard is a leading expert in digital safeguarding and wellbeing with over 20 years' experience working in and with schools. Kat supports schools with developing comprehensive strategies, implementing policies and procedures, conducting training, and establishing committees to promote student safety. Kat's unwavering passion for digital safeguarding and wellbeing drives her to provide expert advice and support on a day-to-day basis
- Tom Newton is a VP of product management at [Smoothwall](#), part of Qoria. Tom has 20 years' experience in making the internet a safer place and is an expert in web filtering technology. Tom is always happy to speak with school leaders about their IT and safeguarding strategies

## Technical Requirements

REQUIREMENT	✓
FILTERING SYSTEM	
Is it a member of the <a href="#">Internet Watch Foundation</a> (IWF)?	<input type="checkbox"/> yes
Is it signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)?	<input type="checkbox"/> yes
Does it block access to illegal content including child sexual abuse material (CSAM)?	<input type="checkbox"/> yes
<p>Are you satisfied that the system manages the following content:</p> <ul style="list-style-type: none"> <li>• Discrimination</li> <li>• Drugs/substance abuse</li> <li>• Extremism</li> <li>• Gambling</li> <li>• Malware/hacking</li> <li>• Pornography</li> <li>• Piracy and copyright theft</li> <li>• Self harm</li> <li>• Violence</li> </ul>	<input type="checkbox"/> yes
<p>Is the filtering system:</p> <ul style="list-style-type: none"> <li>• Operational</li> <li>• Up to date</li> <li>• Applied to all: <ul style="list-style-type: none"> <li>○ Users, including guest accounts</li> <li>○ School-owned devices</li> <li>○ Devices using the school broadband connection</li> </ul> </li> </ul>	<input type="checkbox"/> yes

REQUIREMENT	✓
FILTERING SYSTEM	
<p>Does the filtering system:</p> <ul style="list-style-type: none"> <li>Filter all internet feeds, including any backup connections (e.g. a VPN)</li> <li>Handle multilingual web content, images, common misspellings and abbreviations</li> <li>Identify technologies and techniques that allow users to get around the filtering, such as VPNs and proxy services, and block them</li> <li>Provide alerts when any web content has been blocked</li> </ul> <p>It is:</p> <ul style="list-style-type: none"> <li>Age and ability appropriate for the users, and suitable for educational settings</li> </ul>	<input type="checkbox"/> yes
<p>Does the filtering system allow you to identify:</p> <ul style="list-style-type: none"> <li>Device name or ID, IP address, and where possible, the individual</li> <li>The time and date of attempted access</li> <li>The search term or content being blocked</li> </ul>	<input type="checkbox"/> yes
<p>Are you clear on how long logfile information (internet history) is retained and how it's stored?</p>	<p>(over 6 months)</p> <input type="checkbox"/> yes, checked with Paul 08/05/2024
<p>Are you clear on how the system does not over block access so it doesn't lead to unreasonable restrictions?</p>	<input type="checkbox"/> yes, it blocks some but there is an element of physical monitoring needed. We can set it to overlock but this would restrict education searches.

REQUIREMENT	✓
FILTERING SYSTEM	
<p>Does the filtering system meet the following principles?</p> <ul style="list-style-type: none"> <li>• Context appropriate differentiated filtering, based on age, vulnerability and risk of harm <ul style="list-style-type: none"> <li>○ Can you vary the filtering strength? E.g. for staff?</li> </ul> </li> <li>• Circumvention <ul style="list-style-type: none"> <li>○ Can you identify and manage technologies used to circumvent the system, e.g. virtual personal networks (VPNs), proxy services and domain name system (DNS) over Hypertext Transfer Protocol Secure (HTTPS)</li> </ul> </li> <li>• Control <ul style="list-style-type: none"> <li>○ Can you control the filter yourselves to permit or deny specific content?</li> <li>○ Can you log any changes as part of an audit trail?</li> </ul> </li> <li>• Contextual content filters <ul style="list-style-type: none"> <li>○ 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 artificial intelligence (AI) generated content. For example, being able to contextually analyse text on a page and dynamically filter</li> </ul> </li> <li>• Filtering Policy <ul style="list-style-type: none"> <li>○ Does your provider detail its approach to filtering, as well as over blocking?</li> </ul> </li> <li>• Group/multi-site management <ul style="list-style-type: none"> <li>○ Can your system be deployed centrally, with a central policy and dashboard?</li> </ul> </li> <li>• Identification <ul style="list-style-type: none"> <li>○ Does the system allow you to identify users?</li> </ul> </li> <li>• Multiple language support <ul style="list-style-type: none"> <li>○ Does the system manage relevant languages?</li> </ul> </li> <li>• Network level <ul style="list-style-type: none"> <li>○ Is the filtering provided at 'network level', i.e. it doesn't rely on software on user devices while at school</li> </ul> </li> </ul>	<input type="checkbox"/> yes

REQUIREMENT	✓
FILTERING SYSTEM	
<ul style="list-style-type: none"> <li>• Remote devices <ul style="list-style-type: none"> <li>○ Can the system filter devices where staff and/or pupils are working remotely?</li> </ul> </li> <li>• Reporting <ul style="list-style-type: none"> <li>○ Can you report inappropriate content?</li> <li>○ Does the system provide clear historical information on the websites users have accessed or tried to access?</li> </ul> </li> <li>• Safe Search <ul style="list-style-type: none"> <li>○ Does the system have the ability to enforce 'safe search'?</li> </ul> </li> </ul>	<input type="checkbox"/> yes
<p><b>If users access content via mobile or through apps:</b></p> <p>Get confirmation that your provider can provide filtering on mobile or app technologies.</p> <p>They should also apply a technical monitoring system to devices using mobile and app content to reduce the risk of harm.</p>	<input type="checkbox"/> yes
<p><b>If your filtering provision is procured with a broadband service:</b></p> <p>Make sure it meets the needs of your school or college</p>	<input type="checkbox"/> yes

REQUIREMENT	✓
MONITORING SYSTEM	
Are incidents urgently picked up, acted on and the outcomes recorded?	<input type="checkbox"/>
<p>Are all staff clear on:</p> <ul style="list-style-type: none"> <li>• How to deal with these incidents</li> <li>• Who should lead on any actions</li> </ul>	<input type="checkbox"/>
<p>Is device monitoring managed? (this could be by your IT staff or a third-party provider)</p> <p>Whoever is managing device monitoring will need to:</p> <ul style="list-style-type: none"> <li>• Make sure monitoring systems are working as expected</li> <li>• Provide reports on pupil device activity</li> <li>• Receive safeguarding training including online safety</li> <li>• Record and report safeguarding concerns to the DSL</li> </ul>	<input type="checkbox"/> <p>John Finch Computers could intervene if inappropriate searches continue with pupils or staff members. Particular search terms that keep appearing could be addressed.</p>
Is your monitoring data received in a format that your staff can understand?	<input type="checkbox"/> yes
Are users identifiable to your school or college, so you can trace concerns to an individual, including guest accounts?	<input type="checkbox"/> yes

REQUIREMENT	✓
MONITORING SYSTEM	
<p>Does your monitoring system alert you to behaviours associated with:</p> <ul style="list-style-type: none"> <li>• Content <ul style="list-style-type: none"> <li>○ Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism</li> </ul> </li> <li>• Contact <ul style="list-style-type: none"> <li>○ Being subjected to harmful online interaction with other users; for example: 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</li> </ul> </li> <li>• Conduct <ul style="list-style-type: none"> <li>○ Online behaviour that increases the likelihood of, or causes, harm; for example, 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</li> </ul> </li> <li>• Commerce <ul style="list-style-type: none"> <li>○ Risks such as online gambling, inappropriate advertising, phishing and/or financial scams</li> </ul> </li> </ul>	<input type="checkbox"/> yes



REQUIREMENT	✓
MONITORING SYSTEM	
<p>Does the monitoring system meet the following principles:</p> <ul style="list-style-type: none"> <li>• Age appropriate <ul style="list-style-type: none"> <li>○ Can you vary your strategy to take age, vulnerability, or specific situations (e.g. boarding schools) into account</li> </ul> </li> <li>• Audit trail <ul style="list-style-type: none"> <li>○ Are any changes to the strategy logged so no one can make changes on their own?</li> </ul> </li> <li>• Bring your own device (BYOD) <ul style="list-style-type: none"> <li>○ If your system can monitor staff and pupils' personal devices, make sure this is done according to your data management policies. For example, will your system monitor devices out of school hours?</li> </ul> </li> <li>• Data retention <ul style="list-style-type: none"> <li>○ Be clear on what data is stored, where and for how long (including any backup data)</li> </ul> </li> <li>• Devices <ul style="list-style-type: none"> <li>○ Make sure your system is clear about which devices it covers</li> </ul> </li> <li>• Flexibility <ul style="list-style-type: none"> <li>○ Make it clear how keywords can be added or removed</li> </ul> </li> <li>• Group/multi-site management <ul style="list-style-type: none"> <li>○ Can your strategy be deployed centrally, with a central policy and dashboard?</li> </ul> </li> <li>• Harmful image detection <ul style="list-style-type: none"> <li>○ To what extent is visual content monitored and analysed?</li> </ul> </li> <li>• Impact <ul style="list-style-type: none"> <li>○ How do monitoring results impact your policy and practice?</li> </ul> </li> </ul>	<input type="checkbox"/> yes

REQUIREMENT	✓
MONITORING SYSTEM	
<ul style="list-style-type: none"> <li>Monitoring policy <ul style="list-style-type: none"> <li>How do you tell all users that you're monitoring their online access?</li> <li>How do you communicate your expectations on appropriate use to pupils and staff?</li> </ul> </li> <li>Multiple language support <ul style="list-style-type: none"> <li>Can the system manage relevant languages to your school?</li> </ul> </li> <li>Prioritisation <ul style="list-style-type: none"> <li>How are alerts prioritised?</li> <li>What procedures do you have in place to allow staff to respond to alerts rapidly?</li> </ul> </li> <li>Remote monitoring <ul style="list-style-type: none"> <li>Can the system monitor devices where staff and/or pupils are working remotely?</li> <li>Are users aware of this? Are you clear if these devices are only monitored during school hours?</li> </ul> </li> <li>Reporting <ul style="list-style-type: none"> <li>How are alerts recorded, communicated and escalated?</li> </ul> </li> </ul>	<input type="checkbox"/> Staff meeting for TAs and teachers May 2024
Do your staff: <ul style="list-style-type: none"> <li>Provide effective supervision</li> <li>Take steps to maintain awareness of how devices are being used by pupils</li> <li>Report any safeguarding concerns to the DSL</li> </ul>	<input type="checkbox"/> yes
<b>If users access content via mobile or through apps:</b> Have you applied a technical monitoring system to these devices?	<input type="checkbox"/> yes Staff use apps and webpage that all goes through the filtering

Your school:

- Will need to carry out your own data protection impact assessment (DPIA) and review the privacy notice of third-party providers. [Use this template from the ICO](#)
- Will need to reflect your monitoring procedures in your [acceptable use policy](#)
- May decide to enforce Safe Search or another child-friendly search engine/tool