Highfield CE Primary School

Filtering and Monitoring Policy 2023-2025

Approved by: The governing body	**Date:** 12.10.23
Last reviewed on: **12.10.23**	
Next review due by: **Ocotober 2025**	

Filtering and Monitoring

This policy is based on the Department for Education (DFE's) statutory safeguarding guidance: Keeping Children Safe in Education Document Annex C, and its advice for schools about: Teaching Online Safety in Schools, Preventing and Tackling Bullying, Cyber-Bullying. Advice for Headteachers and School Staff, Searching, Screening and Confiscation and advice published by the UK Council for Online Safety. It should also be read in conjunction with the school's Behaviour Policy, Safeguarding Policy, E-Safety Policy.

Aims

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• Content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• Contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Filters and Monitoring

Highfield CE Primary School uses filtering and monitoring systems that are supplied with the broadband service provided by Coconnect. This system regularly monitors the traffic on the network and the use of certain websites and search topics are restricted.

DSLs are alerted to inappropriate searches via immediate email and can take action appropriately as per the safeguarding/ behaviour policy.

Information and Support for Parent, Staff and Governors

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' evenings, letters, newsletters, website updates, guest speakers and information about e-safety campaigns.

Roles and Responsibilities

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that 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.

The Headteacher

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

The Designated Safeguarding Lead

- 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, 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 child protection policy;
- Ensuring that any online safety incidents are logged (see appendix 5) 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;

• Liaising with other agencies and/or external services if necessary;

• Providing regular reports on online safety in school to the headteacher and/or governing board. This list is not intended to be exhaustive.

The ICT Manager (Harrap)

The ICT Manager (Harrap) is responsible for:

• Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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 a full security check and monitoring the school's ICT systems on a monthly basis;

• Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;

• Ensuring that any online safety incidents are logged 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.

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 of the school's Appropriate Use Policy;

• Working with the DSL to ensure that any online safety incidents are logged) 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'.

Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy;

- Understand that their child has read, understood and agreed to the terms of the school's Appropriate Use Policy.

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

- 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 of the Appropriate Use Policy.

Teaching of Online Safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision and curriculum. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

• A planned e-safety programme will be provided as part of the Computing Curriculum;

• Key e-safety messages are reinforced as part of a planned programme of assemblies and activities;
• Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;

• Pupils will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;

• Through the promotion of British Values and the Prevent Duty the pupils will be taught to challenge extremist views when using material accessed on the internet;

• Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. From the National Curriculum: In Key Stage 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 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. The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Cyber-bullying

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's Behaviour Policy).

Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. 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 cyberbullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information on cyber-bullying to parents so that 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 Examining Electronic Devices – Searching Screening and Confiscation The school will follow guidance from Searching, Screening and Confiscation DfE 2022, UKCIS guidance and school's Behaviour Policy 2022. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure. 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;

• 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 which would violate the school's terms of acceptable use. 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 ICT Manager.

Data Protection

In line with the school's Data Protection Policy, all staff and governors must be aware of the risks posed by data being accessed by unauthorised people. All members of staff and governors must take appropriate steps to minimise this risk by ensuring that all data is kept on password encrypted memory sticks and disposed hard drives are securely destroyed by registered companies when no longer required. Further information can be found on the following websites: www.thinkuknow.co.uk www.disrespectnobody.co.uk www.saferinternet.org.uk www.internetmatters.org www.childnet.com/cyberbullying-guidance www.pshe-association.org.uk http://educateagainsthate.com www.gov.uk/government/publications/the-use-of-social-media-for-onlineradicalisation www.gov.uk/UKCCIS

Examining Electronic Devices – Searching Screening and Confiscation

The school will follow guidance from Searching, Screening and Confiscation DfE 2022, UKCIS guidance and school's Behaviour 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.

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;

• 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 which would violate the school's terms of acceptable use. 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 ICT Manager.

Data Protection

In line with the school's Data Protection Policy, all staff and governors must be aware of the risks posed by data being accessed by unauthorised people. All members of staff and governors must take appropriate steps to minimise this risk by ensuring that all data is kept on password encrypted memory sticks and disposed hard drives are securely destroyed by registered companies when no

longer required. Further information can be found on the following websites:
www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

http://educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-onlineradicalisation

www.gov.uk/UKCCIS

Appendix 1 – Coconnect's filtering procedure's for Highfield CE Primary School

Appropriate Filtering for Education settings

June 2023

Filtering Provider Checklist Reponses

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

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place 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	Coconnect
Address	Harbour House, Hamilton Road, Cosham, Portsmouth, Hampshire, PO6 4PU
Contact details	Email: hello@coconnect.co.uk | Telephone: 02392 322 522
Filtering System	Netsweeper, Smoothwall and FortiGate
Date of assessment	June 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		Netsweeper and Smoothwall are all long standing members of IWF.
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Netsweeper and Smoothwall all block access to illegal Child Abuse Images by actively implementing the IWF CAIC list of domains and URLs.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Netsweeper and Smoothwall block all terrorist content as per the Home Office's terrorism blocklist. It offers unmatched global protection against terrorist and extremist content.
• Confirm that filters for illegal content cannot be disabled by the school		All illegal content categories are locked at a system level. Schools cannot disable these filters.

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.		Netsweeper and Smoothwall have categories that identify websites/content that are intentionally offensive by being discriminatory about race, ethnicity, nationality, gender, sexual orientation, religion, disability or profession.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Netsweeper and Smoothwall block websites/content that feature or encourage illegal drug activities such as the sale, manufacture, distribution or use of drugs and drug paraphernalia. Informational sites featuring information about drugs (such as descriptions, negative effects etc) are not blocked.

Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Netsweeper and Smoothwall categorise and block any websites/content under the 'police assessed list of unlawful terrorist content'. This covers categories including extremism, hate speech, criminal skills, terrorism, and weapons.
Gambling	Enables gambling		Netsweeper and Smoothwall blocks sites that encourage or provide information on gambling (including sites that encourage risking of money on games, contests, and other events. Sites that are strategic or promote cheating are also blocked. Sites for gambling addiction support are not blocked.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Netsweeper and Smoothwall block websites that are associated with malware and hacking. This includes malware, infected hosts, phishing, viruses, and adware.
Pornography	displays sexual acts or explicit images		Netsweeper and Smoothwall block websites/content that contain pornographic images, videos, and text. Websites/content that depict full or partial nudity are also blocked.
Piracy and copyright theft	includes illegal provision of copyrighted material		Netsweeper and Smoothwall block websites that illegally provide copyrighted material or peer-to-peer software.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Netsweeper and Smoothwall block websites/content relating to self-harm, suicide and eating disorders. Websites providing medical information or support are not blocked.

Violence	Displays or promotes the use of physical force intended to hurt or kill		Netsweeper and Smoothwall block websites/content depicting or advocating violence against people and animals. This includes torture, self-inflicted harm, mutilation, suicide, death, gore and injuries.

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

Netsweeper uses a tiered filtering methodology based around dynamic content analysis to accurately categorise these and many other categories. Their AI based technology performs dynamic categorisation of over 90 categories in 47 languages. Netsweeper also has inhouse digital safety and categorisation teams working continuously at improve their categorisation algorithms and lists.

Smoothwall provides filtering and reporting for over 100 other categories ranging from 'Sexuality Sites' and 'Non-Pornographic Nudity' through to 'News', 'Sport' and 'Online Games'. They use a wide variety of techniques to identify and categorise content. All categories use a list of both URLs and domains (with most categories using search terms, content-based rulesets, and regular expressions to identify content quickly). 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.

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

We keep all logfile data for 1 year, as per our retention policy.

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

To ensure over blocking isn't a problem, we regularly review our blocked categories, URLs, and keywords to make sure key educational content isn't blocked. It's very easy for us to unblock and recategorise any blocked categories, URLs, and keywords at the request of the school (so long as it doesn't go against the inappropriate content outlined above.

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		Netsweeper and Smoothwall integrates with existing directory systems (such as Microsoft AD, Azure AD and Google Directory) so filtering

		can be set appropriately at a group and user level. Assigning users to groups means they'll receive appropriate filtering based on their age, vulnerability, or risk of harm.
• 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.		Netsweeper and Smoothwall use advanced technology to detect and prevent any attempts made to circumvent the system.
• Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. 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		Coconnect configures different roles for users. This allows schools to control and maintain the filters and reports themselves. All changes made either by Coconnect or the school are logged for a full audit trail.
• 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.		Netsweeper and Smoothwall analyse and categorise content in real time.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Netsweeper and Smoothwall have their own filtering rationale that includes clear criteria on what should be included (and what should not be) in each category. Care is taken not to over block.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Under Netsweeper's filtering, Coconnect provides a single pane of glass service where policies can be shared across multiple schools. This works in conjunction with reporting, providing hierarchical views for Multi Academy Trusts and federated schools. Under Smoothwall, each school has access to their own interface for reporting

		and to make adjustments to filtering policies.
• Identification - the filtering system should have the ability to identify users		Netsweeper and Smoothwall integrates with existing directory systems (such as Microsoft AD, Azure AD and Google Directory) so different users can be identified and appropriate filtering set accordingly.
• 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		Coconnect utilises Layer 7 application inspection for mobile and application technologies. Layer 7 application filtering is delivered via with Netsweeper and Smoothwall firewalls (depending on deployment method selected by the school).
• Multiple language support – the ability for the system to manage relevant languages		Netsweeper and Smoothwall have extensive directories for multiple languages, as well as human web filtering teams with fluency in multiple languages.
• 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)		Netsweeper and Smoothwall can apply filtering on a network level, so all devices are covered.
• 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		Netsweeper and Smoothwall can apply filtering down to a device level to cover devices on the school network even if it's offsite.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Schools can immediately block/allow access so long as they have an admin role. We also work with designated contacts at the school, to make sure they can report inappropriate content to us. This can be done through our online portal, telephone, or email.
• Reports – the system offers clear historical information on the websites users have accessed or attempted to access		Netsweeper and Smoothwall have their own reporting engines. These allow schools

		to see various reports, data, and alerts
• Safe Search – the ability to enforce 'safe search' when using search engines		Safe Search can be applied for set user groups at the request of the school.

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.

Coconnect focuses on safeguarding and online safety and has a number of different measures in place to educate and support schools in keeping students safe. We provide online guidance for safeguarding through webinars, blog posts, and social media, and are currently producing guides and videos to assist in self-learning. We can also tailor custom messages displayed to students when they try and access blocked content. This means that rather than just blocking a website/page/content, we can educate students and advise where they can get help if they need it.

Netsweeper and Smoothwall also offer a range of additional products for filtering and monitoring that schools can choose to add to enhance their safeguarding solutions.

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	Shayne Grove
Position	Director of Education Services
Date	26/06/2023
Signature