Saint Pierre School,

16 Leigh Road, Leigh-on-Sea, Essex SS9 1LE

ICT Online Filtering and Monitoring Policy

Policy Owner (Position)	Last Updated By (Name)	Date of Last Review	Date Next Review Due	
Headmaster	Peter Lane	19th Dec 24	19th Dec 25	
Read in Conjunction with: ICT Pupil Acceptable Use Policy ICT Acceptable Use Policy Mobile and Smart Technology Policy ICT Online Safety Policy				

Contents

Introduction

Saint Pierre School should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

Aims of this Policy

An active and well managed filtering system is an important part of providing a safe environment for pupils to learn and for staff to work. It is important to recognise that no filtering systems can be 100% effective and needs to be supported with good teaching and learning practice and effective supervision. As such, filtering systems should be recognised as one of the tools used to support and inform the broader safeguarding provision at the school.

Saint Pierre will implement an effective filtering system under the following broad aims:

It Should:

- Block internet access to harmful sites and inappropriate content .
- Ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering.

It should not:

- unreasonably impact teaching and learning or school administration
- restrict students from learning how to assess and manage risk themselves

Related Documentation

4.1 Safeguarding and Child Protection Policy
4.2 Preventing Radicalisation and Extremism Policy
4.3 Promoting Good Behaviour Policy
4.4 ICT acceptable use policy

Roles and Responsibilities

The proprietor/headmaster has the overall strategic responsibility for filtering and monitoring and assurance that the standards are being met.

The DSL is responsible for ensuring these standards are met and takes lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

Our monitoring and filtering provider (Currently STRADCOM) is responsible for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider (Currently Stradcom) should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

The SLT will decide upon (these decisions will be recorded in meeting notes.)

- what is to be filtered and monitored
- Which filtering and monitoring solution to use
- Reviewing the effectiveness of our systems

The SLT is also responsible for ensuring staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Other Staff are responsible for observing use of the system and in particular should report to the Headmaster or DSL if:

Review

For filtering and monitoring to be effective it should meet the needs of our pupils and staff, and reflect our specific use of technology while minimising potential harms.

To understand and evaluate the changing needs and potential risks of our school we will review our filtering and monitoring provision, at least annually or when:

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

The review will be conducted by the Headmaster/Proprietor, DSL and our service provider. The results of the online safety review will be recorded for reference. The review will follow the advice given on reviewing monitoring and filtering in KCSIE 2023.

The review will involve completing the forms in Appendix 1 and 2 and reporting on any issues raised.

Mobile Devices

Pupils may not use school mobile devices unless they are not connected to the internet. Pupils may not use their own mobile devices.

All mobile devices must be inspected by the Headmaster or DSL termly and any unauthorized apps removed.

Mobile devices connected to the school network are all subject to this filtering policy.

Data Protection

The school will need to conduct a data protection impact assessment (DPIA) and review the privacy notices of third party providers annually. A form for the DPIA is in Appendix 3.

APPENDIX 1 – Review of Monitoring and Filtering Tool

This tool along with the technical requirements review (APPENDIX 2) form the full review of our Filtering and Monitoring provision.

Person Completing Review	PL	
Date of Review:	3/11/23	
Staff members overseeing review	GH	
Current filtering provider	DNS Filter inc	
Date effective from	1/11/23	
End of contract	None set	
Current IT specialist	Charlie Ford	
Contact details for above	07348b345263	
Staff leading Filtering and Monitoring with positions	PL – Head GH - DSL	
Have content blocking specific decisions been documented with reasons?	Yes SLT meeting	
Who oversees reports?	Head	
Which reports are scrutinized and how often?	Firewall Breaches Weekly and everytime there is a breach.	
When was the last staff training on the provision. Give details of what was covered.	19/9/24 – what was blocked, how it works and how to react if there is a problem	
Which staff did not attend the training above?	Non academic and some EYFS	
Which senior staff have been trained in the provision by the provider? When was this training?	Head and DSL	
Has a risk assessment been written for the provision. (give date)	Yes – 1/11/23 updated 1/11/24	
Are online safety posters on display in all classrooms?	yes	

APPENDIX 2 – Checklist for Review of Technical Requirements of our Filtering and Monitoring System (Guided by KCSIE 2023)

REQUIREMENT	Compl-iant Y/N	Evidence / Notes	
Filtering Provider			
a member of Internet Watch Foundation (IWF)	Y	Email from provider confirming	
signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)	Y	Email from provider confirming	
blocking access to illegal content including child sexual abuse material (CSAM)	Y		
Is the broadband service, meeting the needs of our school.	Y		
Check the provider's data retention policy and state the length (time) here	Y	3 years	
Filtering System			
Does the school have control of the system?	Y		
Is it up to date?	Y		
Does it apply to all users?	Y		
Does it apply to all school devices?	Y		
Does it apply to all devices using the broadband?	Y		
Does it filter all internet feeds including backup connection?	Y	Tested by ISP	
Does it filter contextual content?	Y	Tested	
Is the illegal content filter unable to be disabled?	Y	Tested	
Is it age appropriate for all users?	Y		
Is it suitable for educational settings	Y	Provider's literature	
Can it filter multilingual content ?	Y	"	
Can it filter images?	Y	"	
Can it filter common misspellings	Y	"	
Can it filter abbreviations?	Y	"	
Does it identify and block technologies used to bypass filtering	Y	Literature with some caution about new tech	

Can it be customized for age or other criteria?	Y	But at the moment we are not doing this we filter for all pupil users at one level and adult users at another.	
Does it filter on mobile devices?	Y	Tested most recently 18/1/24	
Does it filter app content?	?	On laptops but not mobile devices	
Does it identify Device name?	Y?	By IP address	
If an individual attempts to access unsuitable material:			
Does it provide alerts when any web content has been blocked	Y	Y email	
Does it identify IP address?	Y		
Does it identify Device name?	N		
Does it identify the individual?	N	We would need to install AD and are considering this	
Does it identify the date and time of attempted access?	Y	Tested	
Does it identify the search item which has been blocked	Y		
Specific Blocked Content (Test system Laptops)			
Drugs?	Y	Cocaine	
Alcohol	Y	Beer	
Discrimination	Y	Nigger	
Gambling	Y	ladbrokes	
Malware/Hacking	Y	hacking	
Pornography	Y	masterbate	
Privacy and Copyright Theft	Y	Personal details	
Violence	Y	Switch blade	
Self Harm	Y	Wrist cutting	
Illegal Content (Eg CSAM)	Y	Sexual abuse	
Test using tool for the following CSA content, Sexual Content, Terrorist content, Blocks Child Abuse & Terrorist Content).	Y	https://testfiltering.com/	
Specific Blocked Content (Test system Mobile Devices)			
Drugs?	N		
Alcohol	N		
Discrimination	N		
Gambling	N		
Malware/Hacking	N		
Pornography	y		
Privacy and Copyright Theft	N		
Violence	N		
Self Harm	N		
Illegal Content (Eg CSAM)	N		
Test using tool for the following CSA content, Sexual Content,	N	https://testfiltering.com/	

Terrorist content, Blocks Child Abuse & Terrorist Content).			

APPENDIX 4 Filtering and Monitoring Risk Assessment

This Risk assessment covers the risks identified by the tools in appendix 1 and 2

- Review of Monitoring and Filtering Tool
- Checklist for Review of Technical Requirements of our Filtering and Monitoring System (Guided by KCSIE 2023)

These two appendices are part of the risk assessment and help to identify the risks to consider in this assessment.

All F&M systems are not perfect and good teaching practise forms an important part of our F&M at the school.

Risk	Strength H/M/L	Mitigation	
System not 100% effective	M	Teachers trained to monitor screens and behaviour .	
BYOB devices not filtered	L	Not allowed on network. Password changed 1/9/23	
School mobile devices not filtered	M	Teachers required to keep devices away from pupils. Only EYFS staff may use internet in a room with pupils present.	
Policies on filtering in fledgling form and need developing.	M	Have started with consideration of policies provided by AC school	

Last Update of RA : 18/9/23 By: Peter Lane Headmaster

APPENDIX 5 Current Approved List of Banned Sites/Categories

APPENDIX 3 Data Protection Impact Assessment Tool

This template follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

Fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	**Minimal, significant or severe**	**Low, medium or high**

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA