All Saints National Academy

MONITORING AND FILTERING POLICY

Policy Review

This policy will be reviewed in full by the AIB on an annual basis.

The policy was last reviewed and agreed by the AIB on 23/10/23

It is due for review on 23/10/24 (up to 12 months from the above date).

Signature ………………………………….   Date ……………………

Principal

Signature …………………….…………….   Date ….……………………

Chair of AIB

Contents

1. Introduction and overview

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

All Saints National Academy IT service is provided by ICTN Services.

The following information with documentation and responses from Smoothwall and UK Safer Internet Centre references how this is provided.

Our SLT looks after the web filtering for school and will ensure that:

- The service is maintained and accessible for all school sites to use
- All relevant safeguards are being met
- School is taking necessary precautions to ensure the service provided is appropriate
- Also will provide investigation of any web filtering related issues including:
- Access to websites containing inappropriate or potentially harmful material

- Access to websites containing educational or related material deemed appropriate for school
- Provide web access reports on an annual basis

Smoothwall and ICTN works together to ensure that the UK Safer Internet Centre checklist is followed. Smoothwall web filtering service meets and exceeds the Ofsted guidelines. The solution is constantly updated via national feeds from the wider Internet community to ensure that as new websites are created they are categorised and sanctioned accordingly. Above the web filtering aspect of the service, Smoothwall also provide the following features:

- Application Control – this stops some applications running which utilise peer to peer (file-sharing) features
- Intrusion Prevention – this is aimed at stopping hackers from gaining access to your endpoints
- Website Certificate Inspection – this checks websites to ensure any certificates are valid and up to date. This stops users accessing malicious websites or websites that are not properly maintained.

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" (Revised Prevent Duty Guidance: for England and Wales)

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".

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. Children should not be able to access harmful or inappropriate material from the school or colleges 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."

From the information provided to us by our supplier Smoothwall, we are confident that the web filtering solution as configured meets the current DfE guidance.

2. Aims and Objectives

Each school will have its own unique demands and use of the internet. However, all schools must ensure they appropriately safeguard staff and pupils through an effective online filtering and monitoring regime.

3. Requirements of Online Filtering and Monitoring

All schools must ensure that internet systems are robust and appropriate for use.

4. Roles and Responsibilities

The responsibility for the management of the school's filtering and monitoring policy will be held by the E-Safety Coordinator supported by SLT. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the schools filtering service must:

- be logged in change control logs
- be reported to a second responsible person (Headteacher)

All users have a responsibility to report immediately to the E-Safety Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

5. Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the E-Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system. Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, Inset

Parents will be informed of the school's filtering policy through the Acceptable Use agreement.

6. Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the DSL who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered), the E-Safety Co-ordinator should contact head of IT with the URL.

7. Meeting digital and technology standards in schools

7.1/ You should identify and assign roles and responsibilities to manage your filtering and monitoring systems

DSL : James Dean
IT Provider: ICTN
Filtering and monitoring system: Smoothwall

7.2/ You should review your filtering and monitoring provision at least annually Review
Review of filtering and monitoring by DSL and IT provider twice yearly.

7.3/ Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning

See Smoothwall appropriate filtering report

7.4 You should have effective monitoring strategies that meet the safeguarding needs of your school or college

See Smoothwall appropriate monitoring report

7.6/ Filter Test Result

See report of 10/11/2023

8. Links with other policies

This policy will be monitored as part of the school’s annual internal review and reviewed on a three-year cycle or as required by legislature changes. This policy links to the following policies and procedures:

- Safeguarding Policy
- E-Safety Policy

Version Control

As part of the maintenance involved with ensuring this policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains the following information and that all revisions are stored centrally for audit purposes.

Title	All Saints National Academy Filtering And Monitoring Policy 2023
Version	1.0
Date reviewed	23/10/2023
Author	James Dean
Approved by IAB	

Next Review Date	14/06/2026